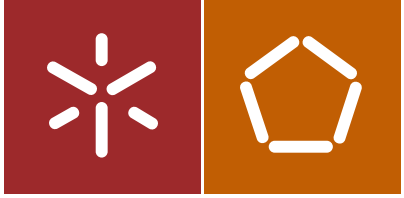
Universidade do Minho
Escola de Engenharia

Maria Manuela Rosas Faria

Métricas para a Gestão do Risco em Segurança da Informação: Caso de Estudo num Centro Hospitalar

Métricas para a Gestão do Risco em Segurança da Informação: Caso de Estudo num Centro Hospitalar
Maria Manuela Rosas Faria
UMinho | 2016

dezembro de 2016



Universidade do Minho
Escola de Engenharia

Maria Manuela Rosas Faria

Métricas para a Gestão do Risco em Segurança da Informação: Caso de Estudo num Centro Hospitalar

Dissertação de Mestrado
Ciclo de Estudos Integrados Conducentes ao Grau de
Mestre em Engenharia Eletrónica Industrial e de Computadores
Especialização em Sistemas de Informação

Trabalho efetuado sob a orientação de
Professor Doutor Henrique Manuel Dinis Santos
Professor Doutor Sérgio Adriano Fernandes Lopes

dezembro de 2016

DECLARAÇÃO

Nome: Maria Manuela Rosas Faria

Endereço eletrónico: mariamanuelarf@gmail.com

Número de Bilhete de Identidade: 14016788

Título dissertação:

Métricas para a Gestão do Risco em Segurança da Informação: Caso de Estudo num Centro Hospitalar

Orientador: Professor Doutor Henrique Manuel Dinis Santos

Co-orientador: Professor Doutor Sérgio Adriano Fernandes Lopes

Ano de Conclusão: 2016

Designação do Mestrado:

Mestrado Integrado em Engenharia Eletrónica Industrial e de Computadores

Universidade do Minho, 29/12/2016

Assinatura: Maria Manuela Rosas Faria

Agradecimentos

Este espaço é dedicado àqueles que, de alguma forma, contribuíram para que esta tese de mestrado fosse realizada. As palavras que aqui deixo pretendem expressar a gratidão para com as pessoas que fizeram parte deste meu trabalho, sendo a ordem de agradecimentos irrelevante, na medida que todos os intervenientes têm um especial lugar de destaque.

Ao Professor Doutor Henrique Manuel Dinis Santos pela sua ajuda, apoio, partilha de conhecimentos e orientação ao longo desta tese de mestrado. Obrigada pela confiança depositada em mim e da concretização do contato com a Engenheira Ana Paula Amorim, do qual surgiu esta dissertação.

À Engenheira Ana Paula Amorim pela sua força de vontade e apoio incondicional ao longo do trabalho, sendo sempre uma figura presente. A energia e entusiasmo que trespassa são contagiantes, revelando-se uma enorme e verdadeira fonte de inspiração e motivação.

Ao Professor Doutor Sérgio Adriano Fernandes Lopes pela sua supervisão e disponibilidade e revisão do trabalho, sendo esta ajuda imprescindível para a finalização do mesmo.

À DigitalSign pela confiança na realização deste trabalho, na disponibilidade dos recursos necessários e pela oportunidade de estagiar com eles. Ao Engenheiro Carlos Fernandes pela sua ajuda na compreensão das normas, disponibilidade para esclarecimento de duvidas e exemplo de grande profissionalismo.

Ao Diretor e Administradores das aplicações em estudo do centro hospitalar onde foi realizado este trabalho, pelos conhecimentos técnicos e científicos que me incutiram ao longo do trabalho, pela colaboração no conjunto de entrevistas que foram realizadas e sem as quais não teria sido possível realizar esta tese de mestrado, pela grande disponibilidade de ajuda, sugestões na melhoria do trabalho e pelas instalações disponibilizadas aquando das idas ao centro hospitalar.

Por último um agradecimento especial aos meus pais, aos meus irmãos e ao Aleksandre por me terem apoiado neste período. Obrigada por todo carinho, amizade, força e compreensão indispensáveis para a existência de um bom ambiente de trabalho e felicidade.

Resumo

Organizações de todos os tipos e tamanhos recolhem, processam, armazenam e transmitem informação reconhecendo que a informação, os processos, os sistemas e as redes são ativos importantes para atingir os objetivos estabelecidos e elas percebem que estes estão inseridos num ambiente de risco. Devido a esta perceção elas implementam controlos de segurança da informação na esperança que estes mitiguem os riscos a que estão expostas, mantenham e aumentem a sua conformidade legal e melhorem a sua imagem. Atividades coordenadas, como apreciações do risco, tratamento do risco e monitorização de processos e sistemas, direcionam a implementação de controlos adequados e tratam riscos de segurança da informação inaceitáveis que são geralmente conhecidos como elementos de Gestão da Segurança da Informação (GSI).

Sendo o foco deste trabalho as organizações do setor da saúde, o problema que elas encontram, é que mesmo não tendo um Sistema de Gestão da Segurança da Informação (SGSI) completamente implementado, elas querem saber a extensão das suas ações. Além de perceberem a eficiência dos controlos implementados, elas procuram que estes modelos possam dar direções sobre ações a seguir e justificar à administração o retorno sobre o investimento (em inglês, *Return on Investment – ROI*) para os controlos implementados na organização e aqueles que podem ser necessários implementar.

Esta dissertação foca-se no estudo da geração de um modelo de métricas de risco da segurança da informação, através de um caso de estudo experimental, num centro hospitalar em Portugal. Para a geração do modelo de métricas é utilizado o modelo apresentado pela ISO/IEC 27004 e os objetos de medição são retirados da apreciação do risco realizada na primeira fase do trabalho, seguindo a norma ISO/IEC 27005. A apreciação do risco foi realizada a um conjunto de cinco aplicações que fazem parte do núcleo funcional do centro hospitalar, estas sendo consideradas como uma boa amostra do sistema e do ambiente da organização e capazes de gerar métricas de risco de segurança da informação eficazes.

As métricas a que se chegou não devem ser consideradas genéricas para as organizações do setor da saúde, mas prevê-se que com este trabalho seja possível perceber uma das metodologias que podem ser usadas para fazer a geração deste tipo de modelos. A abordagem realizada para a geração das métricas mostrou-se eficaz, conseguindo-se chegar a um modelo que foi de encontro às necessidades de informação da organização.

Abstract

Organizations of all types and sizes collect, process, store and transmit information and they acknowledge that the information, processes, systems and networks are important information assets to achieve the objectives that they set and therefore they have a perception that they face a lot of risks that affect the several assets. Due to this perception they implement information security controls in the hope they mitigate the risks they are exposed, keep and increase their legal compliance and improve their image. These activities coordinated, as risk assessment, risk treatment and measure of process and systems, directed the implementation of appropriate controls and they treat unacceptable information security risks generally known as elements of Information Security Management (ISM).

As the focus of this work on the healthcare sector organizations, the problem they face is that despite not having an Information Security Management System (ISMS) fully implemented, they want to know the extent of their actions. In addition to realizing the efficiency of the controls implemented, they seek that these models can give directions on the following actions and justify to management the return on investment (ROI) for the controls implemented in the organization and those that may be necessary to implement.

This dissertation focuses on the study of the generation of a model of risk metrics for information security through a case of experimental study in a healthcare unit in Portugal. For the generation of metrics model is used the model presented by ISO/IEC 27004 and measured objects are taken from the risk assessment made in the first phase of the work, following the ISO/IEC 27005. The assessment of risk was carried out a set of five applications that are part of the functional core of the hospital, these being considered as a good sample of the system and the organization's environment and capable of generating effective risk metrics for information security.

The metrics that was reached should not be considered generic for health sector organizations, but it is expected that this work is possible to see one of the methodologies that can be used to generate this type of models. The approach carried out to generate the metrics proved effective, managing to get to a model that meet the information needs of the organization.

Índice

Lista de Acrónimos

CID	Confidencialidade, Integridade e Disponibilidade
CEO	*Chief Executive Officer*
CIO	*Chief Information Officer*
CIS	*Center for Internet Security*
COBIT	*Control Objectives for Information and Related Technology*
DDoS	*Distributed Denial of Service*
EHR	*Electronic Health Record*
ENISA	*European Union Agency for Network and Information Security*
GSI	Gestão de Sistemas de Informação
GSSI	Gestão da Segurança dos Sistemas de Informação
HIPAA	*Health Insurance Portability and Accountability Act*
IAM	*Identity and Access Management*
ISACA	*Information Systems Audit and Control Association*
ISMS	*Information Security Management System*
ISO/IEC	*International Organization for Standardization/International Electrotechnical Commision*
ITIL	*Information Technology Infrastructure Library*
ITSM	*Information Technology Services Management*
KPI	*Key Performance Indicator*
KRI	*Key Risk Indicator*
NIST	*National Institute of Standards and Technology*
NISTIR	*NIST Interagency or Internal Reports*
PDCA	*Plan-Do-Check-Act*
PHI	*Personal Health Information*

RES	Registo Eletrónico de Saúde
RGPD	Regulamento Geral de Proteção de Dados
ROSI	*Return on Security Investment*
SANS	*System Administration Networking and Security*
SGSI	Sistema de Gestão de Segurança da Informação
SI	Sistema de Informação
SLA	*Service Level Agreement*
TI	Tecnologias de Informação

Lista de Figuras

Lista de Tabelas

Glossário

Além dos termos e definições que podem ser encontrados no Apêndice 2, aqui serão apresentados os conceitos que estarão na base desta tese de mestrado e que devem ser considerados durante a leitura da mesma:

Ameaça: causa potencial de um incidente indesejável, o qual pode causar perigo a um sistema ou à organização [1].

Análise do risco: processo destinado a compreender a natureza do risco e a determinar o nível do risco [2].

Apreciação do risco: processo global de identificação do risco, análise do risco e de avaliação do risco [2].

Atributo: qualquer coisa que tem valor para a organização.

Auditoria de gestão do risco: processo sistemático, independente e documentado de obtenção de evidências e sua avaliação objetiva de forma a determinar o grau de adequação e eficácia de uma estrutura de gestão do risco, ou de uma parte selecionada desta [2].

Confidencialidade: proteção da informação contra o acesso a esta por utilizadores não autorizados [3].

Controlo: medida que modifica o risco [2].

Disponibilidade: habilidade dos utilizadores finais tirarem benefícios do sistema [3].

Gestão do risco: atividades coordenadas para dirigir e controlar uma organização no que respeita ao risco [2].

Integridade: proteção da informação contra modificação não autorizada [3].

Métrica: uma medição, feita sobre um período de tempo, que comunica informação vital sobre um processo ou atividade. Uma métrica deve levar à tomada de ações apropriadas por parte dos líderes ou administradores [4].

Monitorização: verificação, supervisão, observação crítica ou a determinação do estado de modo a identificar continuamente alterações do nível de desempenho requerido ou esperado [2].

Partes interessadas: pessoa ou organização que pode afetar, ser afetado ou sentir-se afetado por uma decisão ou atividade [2].

Processo de gestão do risco: aplicação sistemática de políticas, procedimentos e práticas de gestão às atividades de comunicação, consulta, estabelecimento do contexto e identificação, análise, avaliação, tratamento, monitorização e revisão do risco [2].

Risco: efeito da incerteza na consecução dos objetivos [2]. Probabilidade de ocorrência de uma ameaça ou ataque que explora a vulnerabilidade do ativo.

Segurança: no seu significado mais básico é a proteção de ou a ausência de perigo [5].

Vulnerabilidade: propriedades intrínsecas de algo que resultam na suscetibilidade a uma fonte de risco que pode conduzir a um evento com uma consequência [2].

1. Introdução

Esta seção aborda a motivação, a contribuição que este trabalho transfere à comunidade científica na área das métricas de risco da segurança da informação e quais são os objetivos que são atingidos, sendo estes abordados na parte final do trabalho.

Esta dissertação foi escrita principalmente com uma perspetiva de gestão/governação da segurança da informação dentro de uma organização, pois considerar só a parte tecnológica do seu ambiente é limitado quando se pretende fazer a gestão de risco de toda uma organização. A informação faz parte de qualquer sistema quer ele seja completamente tecnológico ou ainda não esteja completamente desmaterializado e está em contato com os vários intervenientes da organização. Numa era onde se procura a desmaterialização completa dos sistemas de forma a melhorar os processos e o fornecimento dos serviços aos clientes, a questão da segurança da informação é cada vez mais importante, devido a existência de grandes volumes de informação armazenada eletronicamente permitindo que esta seja facilmente acessível remotamente ou localmente. As organizações estão a ficar cientes dos riscos que correm e as pessoas estão cada vez mais conscienciosas sobre a informação que entregam esperando assim que a organização invista na segurança aplicando os controlos necessários para proteger a informação.

Este trabalho começou através da parceria com a DigitalSign, empresa de segurança eletrónica, estando em destaque a sua atividade de Entidade Certificadora Portuguesa para a emissão de certificados digitais qualificados. Sendo uma empresa que trabalha na área da segurança da informação, está empenhada em perceber a orientação que outras organizações (outros setores de atuação) têm neste campo. Assim, tendo ela contato com um centro hospitalar que mostrou interesse em evoluir a sua organização na área da segurança da informação, surgiu este trabalho com um cariz muito prático e capaz de trazer à comunidade científica e profissional o panorama da realidade das organizações que trabalham no setor da saúde em Portugal face à segurança da informação.

O desafio lançado pelo centro hospitalar incluía a análise de uma parte do ambiente operacional da organização de forma a gerar um modelo de métricas de risco da segurança da informação que fosse aplicado nesse contexto. O objetivo do centro hospitalar é ter um modelo de métricas que os profissionais responsáveis pela segurança ou que tenham de reportar sobre a mesma, possam demonstrar o que está feito e como isso está a proteger

a organização, qual é a conformidade face ao Regulamento Geral de Proteção de Dados (RGPD) [6] e que ações deveriam ser consideradas de seguida.

A segurança de computadores tem aumentado em prioridade para muitas organizações e o investimento em segurança de TI tem aumentado significativamente em certos setores. A segurança está-se a tornar cada vez mais num ponto principal não só para o investimento, mas também para o escrutínio do retorno sobre esse investimento. Em face aos regulares relatórios de fugas de informação, sendo exemplos destes relatórios os documentos [7] e [8], os gestores de segurança estão, agora mais que nunca, a serem obrigados a demonstrar a eficácia dos seus programas de segurança [9].

É necessário existir uma maneira de avaliar a eficácia do trabalho realizado, identificar deficiências, e priorizar ações quanto a controlos a implementar ou de controlos já implementados. É necessária uma maneira de facilitar as tomadas de decisão, melhorar o desempenho e a responsabilidade através da recolha, análise e apresentação de informação necessária capaz de avaliar o sistema e a organização. Em segurança da informação há muitos processos que precisam de ser medidos, para que o desempenho dos controlos, dos profissionais e da administração, seja verdadeiramente demonstrável. É necessário saber o quão efetivos e eficientes são os controlos de segurança, não só para ter a certeza que os ativos estão devidamente protegidos, mas também para assegurar que a organização está a ser responsável financeiramente quanto aos esforços orçamentais [10].

Regulamentos como o RGPD requerem que as todas as organizações que tratam de informação de cidadãos europeus, o que inclui neste caso as organizações de saúde em Portugal e nos outros países membros da União Europeia (EU), implementem controlos organizacionais, físicos e lógicos que assegurem a integridade e a privacidade dos registos dos pacientes e outros dados médicos sensíveis. As organizações de saúde são um alvo para os cibercriminosos devido à riqueza que possuem os dados pessoais de saúde, pois estes poderão ser altamente rentabilizados. A questão é se os regulamentos sozinhos serão capazes de parar a realidade difícil que é uma rede bem-sucedida de criminosos voltando-se para o setor da saúde [11]. As organizações querem entrar em conformidade com eles e assim proteger o seu sistema, mas será que o sabem fazer da melhor forma e de forma a que se consiga obter os maiores benefícios possíveis, tendo em consideração o ambiente, o sistema, o orçamento e os colaboradores.

1.1 Motivação

"A segurança e a privacidade da informação dos pacientes são preocupações para todas as organizações de saúde" [12]. Virtualmente todos os *softwares*, aplicações e dispositivos estão neste momento conectados à Internet e esta é uma realidade que os cibercriminosos reconhecem e estão a explorar para obter mão da informação que está armazenada nestes [13].

A importância de assegurar a segurança dos ativos de informação está-se a tornar mais crítica a cada ano e dessa forma discussões sobre as questões de segurança da informação são necessárias para que organizações se tornem conscientes disso. Contudo, as áreas chaves da gestão do risco da segurança da informação e métricas de risco da segurança da informação não têm recebido muita atenção [12].

A maioria das organizações a nível nacional está a olhar pela primeira vez para este tipo de questões, pelo que é importante perceberem qual é o rumo a seguir. Pode ser frustrante para as organizações seguirem um plano restrito seguindo uma determinada norma ou regulamento, antes de terem perceção do que realmente estão a fazer de bem quanto aos controlos já implementados a nível da segurança da informação. Por um lado, querem perceber quais os riscos que estão a correr de forma a fazerem uma análise do risco para perceberem que ações devem tomar para diminuir o mesmo, por outro querem perceber se os controlos já implementados estão a criar valor para a organização, protegendo a informação.

Neste sentido, as organizações de saúde estão a olhar para algumas normas na área da segurança da informação e estão interessadas em estudos que mostrem benefícios que podem advir da implementação dessas mesmas normas. Este trabalho surgiu enquadrando-se nesses estudos e a família de normas escolhida para verificar a sua implementação foi a ISO/IEC 27000. Esta norma é particularmente interessante, pois tem uma norma especialmente direcionada para o setor da saúde, a ISO/IEC 27999.

Muitas organizações compreendem mal os conceitos fundamentais por trás da ISO/IEC 27001 e dessa forma têm-na tratado como um exercício de *marketing*, ao contrário de tentarem atingir benefícios reais para os processos e o retorno sobre o investimento [13]. Este trabalho mostra como se pode usar esta norma de forma a tirar benefícios dela, através da utilização conjunta da ISO/IEC 27005 e a ISO/IEC 27004, atingindo assim métricas para a gestão do risco em segurança da informação.

A tarefa de geração de métricas é considerada uma tarefa direta, porque a maior parte dos departamentos de TI já trabalharam ou estão a trabalhar com alguma ferramenta de medição na sua organização. O conhecimento desta situação pode levar a pensar que eles saberão como medir a segurança da informação nas suas organizações, assim como fornecer valor sobre o orçamento investido em segurança da informação quando em reunião com as partes interessadas e acionistas.

Entre as ferramentas de medição mais usadas pode-se encontrar:

- ***Service Level Agreement (SLA)***: contrato entre um fornecedor de serviços de Tecnologia de Informação (TI) e um cliente ou organização especifica, em geral em termos mensuráveis, sobre quais serviços o fornecedor vai prestar. Níveis de serviço são definidos no início de qualquer relação de *outsourcing* e usados para medir e monitorizar o desempenho de um fornecedor;
- ***Information Technology Infrastructure Library (ITIL)****:* o objetivo com as métricas é fornecer uma ferramenta que alinha o departamento de TI com os objetivos de negócio. Esses objetivos depois criam valor através de melhoria contínua e o ciclo de medição é centrado no ciclo *Deming*, PDCA.

Mas o pensamento está errado, pois toda a área de como e "o que é uma boa e efetiva segurança da informação está frequentemente mal construída, má comunicada e, pior que tudo, mal gerida" [13]. E isto é importante, porque saber o que se está a passar, ter informação que permita garantir conhecimento sobre o sistema e transparência com a gestão, são metas que as organizações tentam alcançar [14].

Um outro tópico muito importante, é o RGPD que foi tornado lei este ano e que dará às organizações, que tratam dados de cidadãos europeus, dois anos para que o apliquem. As organizações do setor da saúde terão de entrar em conformidade com ele e consequentemente ter meios de apresentar as ações e as decisões tendo este regulamento por base.

As métricas não são explicitamente obrigatórias nas organizações em Portugal, mas através do RGPD podemos encontrá-las implicitamente quando se verifica que o responsável pelo tratamento dos dados que neste caso, é o centro hospitalar, tem de mostrar que as decisões tomadas estão a ir de encontro ao RGPD. Neste sentido as métricas são uma boa ferramenta para demonstrar o trabalho que está a ser realizado.

Considerando o RGPD, a pouca preparação por parte das organizações para usar efetivamente ferramentas de medição da segurança da informação e a perceção dos riscos que envolvem a informação confidencial com que lidam diariamente esta é uma área de investigação importante. Para que as organizações se possam proteger contra os riscos que surgem à volta da informação que recolhem, analisam, trabalham e armazenam, é necessário que elas conheçam as vulnerabilidades do seu sistema, apreciação do risco, tomem ações que mitiguem os riscos, tratamento do risco e monitorizem o sistema para avaliar os controlos implementados, métricas para a gestão do risco da segurança da informação. Não se pode pensar que se houver fugas de informação intencional ou não intencional, é só uma divulgação de informação, porque uma das consequências da ocorrência de um determinado incidente é a diminuição da reputação da organização que consequentemente causa um grande impacto negativo ao seu negócio.

1.2 Contribuição para a Área das Métricas

Os principais resultados desta tese de mestrado são:

- Um caso prático da aplicação de uma apreciação do risco, baseada na ISO/IEC 27005, onde é apresentada a metodologia que foi seguida e que se pode analisar no Apêndice 2;
- Um caso prático da aplicação da geração de métricas para a gestão do risco da segurança da informação, baseada na ISO/IEC 27004, a um centro hospitalar e ao seu sistema;
- Um levantamento de métricas para cada um dos controlos recomendados ou utilizados no hospital aquando da apreciação do risco e que se enquadram no ambiente organizacional do centro hospitalar em estudo;
- Um conjunto de métricas para a gestão do risco da segurança da informação gerado a partir da necessidade de informação e facilidade de obtenção dos dados para gerar ou instanciar às métricas;
- Uma avaliação da usabilidade e da viabilidade de gerar um modelo de geração de métricas de risco, onde os objetivos de medição são extraídos da apreciação do risco.

Pretende-se contribuir para esta área mostrando a importância de existir um mapeamento das relações entre os riscos organizacionais e as ações que fazem parte do SGSI (em inglês, *Information Security Management System - ISMS*) da organização. O que acontece

na maioria das organizações é olhar para a ISO/IEC 27001 e focar-se somente em assegurar que a organização tem todos os controlos especificados por ela implementados. Dessa forma esquecem-se de analisar e ligar essa implementação com os verdadeiros riscos que a organização enfrenta. Numa altura em que é necessário mostrar o retorno sobre o investimento feito a nível da segurança da informação (em inglês, *Return on Security Investment* - ROSI), é necessário que as organizações, quer sejam da área da saúde ou de outra área percebam que de nada vale ter os controlos lá implementados se estes não são verdadeiramente necessários.

1.3 Objetivos da Dissertação

Os objetivos que se pretendem atingir com este trabalho são os seguintes:

1. Apresentação de um modelo de métricas onde o processo de análise do risco define as variáveis críticas que quando monitorizadas podem auxiliar a geração de métricas para a gestão do risco;
2. Aplicação prática do método apresentado pela ISO/IEC 27004 para a geração de métricas de risco de segurança da informação;
3. Mostrar as dificuldades que as organizações do setor da saúde podem enfrentar ao tentar construir um modelo de métricas;
4. Dar uma imagem do que é possível na prática ser feito a nível da geração de métricas de risco de segurança da informação nos centros hospitalares em Portugal e do esforço requerido para que elas tenham usabilidade e viabilidade dentro da organização;
5. Um conjunto de métricas baseado na necessidade de informação envolvendo a habilidade de obter a informação requerida assim como a habilidade de produzir resultados adequados para as partes interessadas da organização.

Um dos objetivos mais importantes e no qual o objetivo 1 e o objetivo 2 podem ser agrupados, é mostrar a importância de se realizar uma apreciação do risco, e o modelo de métricas nascer a partir dessa documentação. Segundo [13], as maiores lacunas são geralmente encontradas à volta da documentação que devia estabelecer as relações entre os riscos identificados e que controlos estão implementados e porquê, estas nascendo de um mau entendimento de qual é a verdadeira essência da ISO/IEC 27001, que é a gestão do risco. Este objetivo baseia-se no seguinte: “Métricas de segurança são as servas da gestão do risco, e a gestão do risco é sobre tomadas de decisão. Portanto, as únicas

métricas em que se está interessado são aquelas que suportam a tomada de decisão feita sobre o risco com o intuito de o gerir" [15].

1.4 Estrutura do Documento

Este trabalho está dividido em quatro capítulos que estão estruturados da seguinte forma:

1. **Enquadramento teórico:** apresenta em mais detalhe alguns dos conceitos usados, analisa a área da segurança da informação no setor da saúde em Portugal e faz um enquadramento à família de normas ISO/IEC 27000, descrevendo as normas que foram consideradas para o desenvolvimento deste trabalho. Desenvolve os conceitos de segurança de informação, SGSI e métricas de segurança da informação, incluindo dentro do conceito de métrica as diferenças entre *Key Performance Indicator* (KPI) e *Key Risk Indicator* (KRI). Neste capítulo é também apresentada a revisão bibliográfica a trabalhos existentes na área das métricas de segurança;
2. **Metodologia:** esta seção aborda em detalhe a metodologia seguida nas três partes do trabalho e dessa forma está dividida em três seções. A primeira seção aborda a metodologia seguida na apreciação do risco. A segunda seção aborda o levantamento de métricas realizado para os controlos que foram recomendados, tendo como base a informação recolhida sobre o ambiente do centro hospitalar. A terceira seção aborda a geração de métricas para a gestão do em segurança da informação, o que deve ser feito, como deve ser feito e avalia se elas são realmente importantes para a organização;
3. **Resultados:** neste capítulo estão agrupados os resultados obtidos durante as três partes do trabalho. A primeira seção do capítulo apresenta os resultados obtidos durante a apreciação do risco. Na segunda seção para cada um dos controlos recomendados é feita uma análise em contexto hospitalar e é apresentado o levantamento de métricas realizado. Na terceira seção apresenta-se as métricas escolhidas que fazem parte do modelo de métricas para a gestão do risco em segurança da informação;
4. **Conclusões:** este capítulo apresenta uma visão sobre o modelo de métricas para a gestão do risco em segurança da informação gerado, abordando se estas estão em condições de serem postas em prática e se a sua recolha cria valor para a organização.

2 Enquadramento Teórico

Neste capítulo pretende-se fazer uma introdução teórica a todo o trabalho realizado. Os conhecimentos expostos devem ser considerados de forma a se perceber e compreender o restante trabalho.

2.1 Exploração de Conceitos: Segurança da Informação e Métrica de Segurança

De forma a termos a correta interpretação do trabalho, é necessário perceber o que realmente foi considerado ao longo deste como sendo a definição de segurança da informação e métrica de segurança da informação. Na parte inicial do documento podemos encontrar um pequeno glossário com as palavras chaves, no entanto nesta seção procura-se dar uma visão mais alargada dos conceitos usados.

Quanto à segurança da informação, de acordo com [12], esta é um processo de garantia da confidencialidade, integridade, disponibilidade, autenticidade e não repúdio para uma entidade de acordo com alguma política. Isso protege a informação e os sistemas de informação de acesso não autorizado, uso, divulgação, rutura, ação de ler ou examinar, gravação ou destruição. O termo segurança da informação é geralmente baseado na informação, sendo esta considerada como o ativo mais importante das organizações na era atual, a qual tem um valor e requer uma proteção apropriada contra a perda de confidencialidade, integridade e disponibilidade. Buscando a eficácia dos processos da organização, a informação tem de ser exata, estar completa e disponível em tempo útil para que utilizadores autorizados a possam aceder consoante a sua necessidade e de acordo com a sua profissão, onde lhe será atribuído determinado perfil de utilizador.

Quanto à definição de métrica de segurança, a definição usada durante este trabalho está exposta no Glossário. Mas há muitas outras definições que são estabelecidas por outros autores e que no fundo acabam por completar a definição das métricas de segurança da informação. Com a análise das várias definições de métricas, espera-se abrir já aqui um pouco do estado da arte desta área.

De acordo com Deswarte [13], as métricas consistem num grupo de ferramentas conectadas com vista a atingirem características particulares e níveis de segurança consoante os objetivos da organização. Em [16] encontra-se que as métricas podem responder à questão de qual é a qualidade e adequação das políticas e dos procedimentos

implementados. Por outro lado em [17], o termo métrica é considerado um sistema de transformação e apresentação apropriada para fazer relatórios apresentados à administração. De acordo com [9], métricas de segurança são uma coleção de várias medidas feitas em diferentes pontos no tempo, comparadas contra uma linha de base e interpretadas para obter informação necessária para a organização. De acordo com Brotby [5], as métricas são um termo usados para denotar uma medição baseada numa referência e envolve pelo menos dois pontos, a medição e a referência. A métrica de segurança deve demonstrar o estado ou grau de segurança relativamente ao ponto de referência e o que está a ser feito para evitar o perigo. Este último autor enfatiza que as métricas existem somente para fornecer suporte à tomada de decisão e a informação que elas fornecem é somente útil na extensão que serve este propósito.

Em [15], podemos encontrar um dos objetivos mais amplamente aceites em relação às métricas de segurança, sendo este a quantificação da informação para facilitar o conhecimento.

De todas estas definições expostas e adotadas pelos diferentes autores, pode concluir-se que ainda não foi encontrada uma definição clara e muitas vezes estas mesmas definições de métricas de segurança da informação baseiam-se em como elas são usadas ou por características ou atributos que as tornam úteis [18].

Também relacionado com o campo das métricas, podemos encontrar em [15] o estabelecimento do que são boas métricas. O autor defende que boas métricas são aquelas que permitem medições constantes sem que haja critérios subjetivos e usem poucos recursos para que a recolha da informação tome lugar, se possível de forma automática. Estas devem ser expressas como um número cardinal ou percentagem, expressas com pelo menos uma unidade de medida e especificamente contextualizadas e relevantes para os administradores.

Neste contexto de métricas de segurança é também importante perceber a diferença entre métricas, *Key Performance Indicator* (KPI) e *Key Risk Indicator* (KRI), pois estes conceitos são muitas vezes confundidos. Considera-se como métrica tudo aquilo que se pode medir, sendo que o resultado dessa medição irá determinar se este é um KPI ou um KRI. Quando uma métrica reflete o alcance de um objetivo desejado, esta pode-se tornar um KPI do processo avaliado dentro de uma área específica da organização. Na situação

contrária, quando a métrica fornece informações de exposição a riscos numa área concreta de operações, esta pode-se tornar um KRI.

2.2 Segurança da Informação e o Setor da Saúde

A segurança da informação é uma questão de negócio e deve ser tratada como tal. Esta deve ser adequadamente integrada nas metas e objetivos de negócio da organização, pois as questões de segurança podem afetar negativamente os recursos de que depende para prestar os seus serviços. O preço que se tem de pagar quando a segurança não recebe a atenção, suporte e fundos apropriados está a tornar-se uma preocupação para as organizações [10].

O setor da saúde tem muita informação que pode ser valiosa para os cibercriminosos, o que o faz alvo de ataques constantes de forma a conseguir obter essa informação. A regularidade destes ataques deve-se ao fato deste setor somente agora começar a se preocupar em proteger o seu sistema para assegurar quer a segurança da informação, como a segurança física dos pacientes. E eles têm que ser rápidos pois todas os processos deste setor dependem cada vez mais dos Registos Eletrónicos de Saúde (RES) para prestarem os serviços. A desmaterialização de processos está a ter um papel importante na mudança de mentalidade sobre a segurança da informação, por parte das organizações.

Fazendo referência a [19], a qualidade dos diagnósticos e tratamentos de saúde dependem fortemente da informação sobre a condição dos pacientes. Os RES são a forma atual de armazenar informação e em tendo em atenção os principais princípios de segurança, CID, é fácil verificar o porquê de estes serem essenciais para os sistemas de RES. Como os RES contêm informação que é considerada altamente sensível pois contem informação pessoal de pacientes, há uma extrema necessidade de confidencialidade. A integridade é essencial uma vez que um tratamento baseado em informação médica errada pode ser fatal e quanto à disponibilidade esta é essencial porque a informação nos RES tem de ser acedida pelo profissional de saúde para que haja um tratamento adequado em tempo útil [19].

Em termos de capacidades técnicas, a indústria da saúde está atrás, por exemplo da indústria financeira ou de desenvolvimento tecnológico, em relação à proteção das suas infraestruturas e informação confidencial dos pacientes (em inglês, *Electronic Protected Health Information - ePHI*). Este setor é normalmente associado com o uso de tecnologia clínica desatualizada, dispositivos médicos para acesso à rede inseguros e uma completa

falta de processos de gestão de segurança da informação. A magnitude das ameaças contra a informação do setor da saúde tem crescido exponencialmente, mas a intenção e/ou o investimento em proteger essa informação não tem conseguido parar esse crescimento [8].

Dessa forma as organizações estão a pensar em cibersegurança e na sua forma de gestão que inclui os riscos que envolvem a informação. Tendo isto como pano de fundo, pode-se afirmar que esta pode trazer vários benefícios a uma organização, sendo o mais importante a evolução da cibersegurança como sendo uma questão tecnológica e passar a ser uma questão de gestão. Os quadros de administração começam a sentir a necessidade de entender as implicações legais dos riscos que envolvem a informação que armazenam e manter ligações com especialistas em cibersegurança em intervalos de tempo predefinidos e regulares de forma a ajudar a organização.

2.3 Família de Normas ISO/IEC 27000

Através do uso da família de normas ISO/IEC 27000, as organizações podem desenvolver e implementar uma estrutura para gerir a segurança dos seus ativos de informação. Estes podem incluir informação financeira, propriedade intelectual e detalhes de colaboradores, ou informação que lhes é confiada pelos seus clientes ou terceiros [1].

Esta família é baseada no risco e especifica as melhores práticas e os controlos de segurança mais completos para a gestão da segurança da informação dentro de uma organização.

Para o trabalho descrito nesta dissertação, é necessário destacar as quatro normas específicas que foram utilizadas e sobre as quais o trabalho foi desenvolvido, sendo estas descritas nas subseções seguintes. De destacar que na descrição de cada uma das normas se evidenciará o que realmente foi usado para o desenvolvimento deste trabalho.

Na família de normas ISO/IEC 27000 pode-se encontrar um conjunto de objetivos de controlo, os quais podem ser escolhidos para a organização. Esses objetivos frequentemente incluem a garantia de confidencialidade, integridade e disponibilidade dos ativos da organização [12].

2.3.1 ISO 27001 – *Information security management systems: Requirements*

Nesta norma pode-se encontrar os requisitos que devem ser seguidos pela organização de forma a implementarem um SGSI que realmente previne os riscos que podem rondar os ativos de uma organização.

A ISO/IEC 27001 apresenta um método normativo para criar, implementar e operar um SGSI. Adicionalmente, a norma prescreve um conjunto adequado de metas de segurança da informação, as quais, se devidamente cumpridas, proporcionam confiança para a área da segurança da informação da organização [20]. De acordo com a mesma, um número de ações deve ser tomado quando um SGSI está para ser implementado. Citando novamente [20], exemplos de ações podem ser: definir uma política de segurança da informação, conduzir uma apreciação do risco, priorizar entre riscos identificados e abordar os riscos de uma maneira intencional e controlada.

Esta norma prescreve um conjunto de 114 controlos de segurança da informação que devem fazer parte de um SGSI. Esses controlos estão divididos em 14 grupos e há 35 objetivos de controlo. Esses controlos podem ser implementados quer façam parte ou não de um SGSI, mas considerando a certificação, para que uma organização seja certificada a exclusão de um determinado controlo requer justificação. De acordo com a ISO/IEC 27001, as organizações não precisam de ter a implementação de todos os controlos, mas sim a documentação do porquê da implementação de determinado controlo e a não implementação de outros. Adicionalmente, o impacto dos controlos deve ser medido regularmente para assegurar que eles estão em linha com os objetivos da organização e que esses objetivos estão a ser atingidos. Uma descrição de como realizar essas medições não está incluída na norma ISO/IEC 27001, mas encontra-se descrita na norma ISO/IEC 27004.

A escolha da ISO/IEC 27001, deve-se ao facto da norma oferecer à organização uma sólida, ainda que flexível, estrutura de trabalho de base, para que haja uma gestão efetiva da segurança da informação dentro da organização. Esta é uma norma baseada no risco dos ativos e não nos ativos em si.

A norma ISO/IEC 27001 para a gestão da segurança da informação foi publicada em 2005, tendo esta sido revista em 2013. De acordo com [20], desde que foi publicada, esta tem sido amplamente aceite como uma ferramenta para atingir com sucesso programas em segurança da informação por parte das organizações.

Milhões de entidades no mundo utilizam as práticas documentadas nesta norma e usufruem dos benefícios da sua adoção, sendo que, as entidades que assim o desejam podem também certificarem-se, demonstrando assim de forma adequada que cumprem os requisitos que constam na mesma e a proteção da informação que tratam.

Neste trabalho esta norma foi usada para saber que controlos se enquadravam na mitigação dos riscos, encontrados na apreciação do risco. Foi também a análise desta norma que permitiu fazer o primeiro levantamento de perguntas, que pode ser consultado na Tabela 18, e que foram colocadas aos administradores das aplicações em estudo. Sabendo os requisitos que uma organização deve cumprir para conseguir ter um bom SGSI implementado, é fácil perceber aquilo que se deve procurar dentro do sistema da organização e dessa forma compreender o contexto dos controlos até agora implementados.

2.3.2 ISO 27002 – *Information technology – Security techniques – Code of practice for information security controls*

A norma ISO/IEC 27002 foi originalmente publicada como a renomeação da norma original ISO/IEC 17799, código de prática para a segurança da informação. Ela esboça para cada um dos controlos contidos, na ISO/IEC 27001, orientações de implementação e, desenvolve quando necessário, uma explicação mais detalhada do controlo, por essa razão a ISO/IEC 27001 e a ISO/IEC 27002 estão destinadas a ser usadas juntas, de forma a se completarem uma à outra [21].

A norma, de acordo com [22], "estabelece diretrizes e princípios gerais de iniciação, implementação, manutenção e aperfeiçoamento da gestão da segurança da informação dentro da organização. Os controlos atuais listados na norma destinam-se a endereçar os requisitos específicos identificados através de uma apreciação do risco formal. Ela também se destina a fornecer um guia de desenvolvimento de "normas de segurança organizacionais, práticas de gestão de segurança efetiva e de orientações para ajudar a trazer confiança às atividades internas da organização" [22].

Esta norma foi estudada para criar o segundo conjunto de perguntas feitas aos administradores, que pode ser consultado na Tabela 19. Devido a esta norma ser mais específica quanto às ações que devem ser tomadas para se implementar determinado controlo, ela permitiu estabelecer um conjunto de perguntas de cariz mais tecnológico sobre os processos estabelecidos no centro hospitalar.

2.3.3 ISO 27004 – *Information technology – Security techniques – Information security risk management*

Esta norma internacional fornece uma explicação de medidas e atividades de medição que são precisas para avaliar a eficácia dos requisitos de um SGSI que são necessários para a gestão adequada e proporcional dos controlos de segurança exigidos na norma ISO/IEC 27001.

A norma ISO/IEC 27004, preocupa-se com o desenho e uso de um programa de métricas em segurança da informação. Para criar tal programa, as métricas (chamados modelos de construção na ISO/IEC 27004) são criadas para os controlos que estão incluídos no SGSI de uma organização.

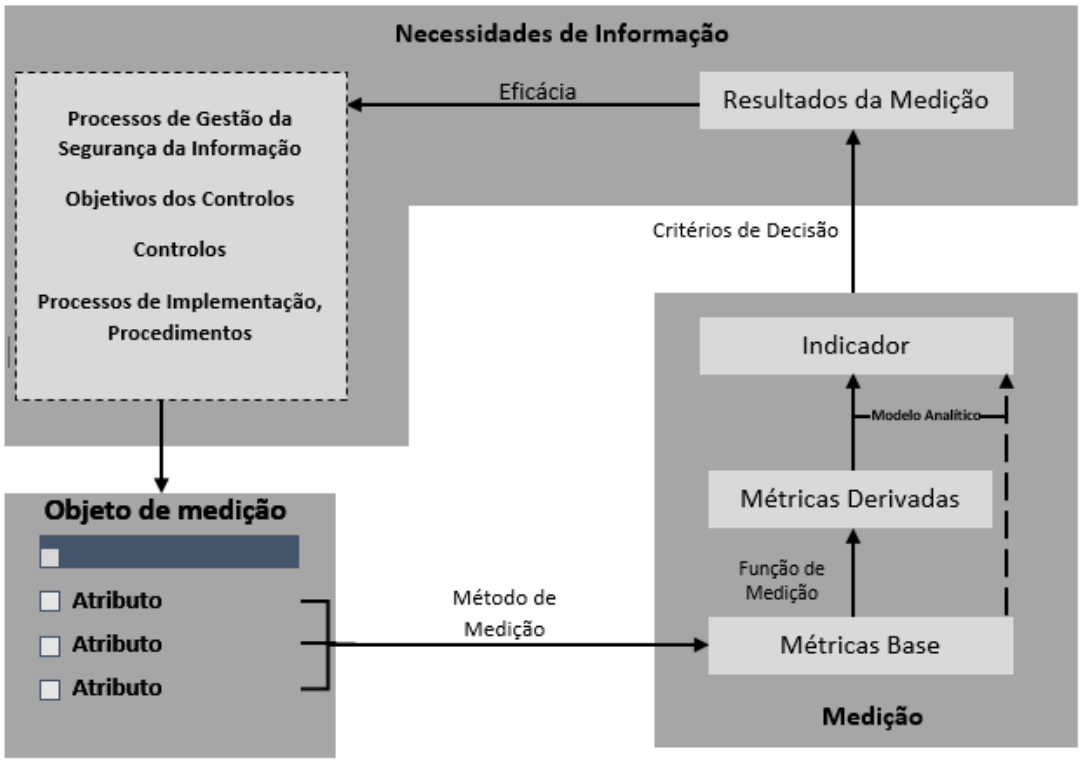


Figura 1. Modelo de medição da segurança da informação apresentado pela ISO/IEC 27004 [23]

Embora sendo assumido na ISO/IEC 27004 que há um SGSI implementado na organização, como descrito na ISO/IEC 27001, não há nada que impeça uma organização de utilizar o modelo descrito na ISO/IEC 27004, para gerar métricas para medir aspetos e necessidades da segurança da informação, definidos pela organização.

O processo para a geração de uma métrica de acordo com esta norma, está apresentado na Figura 1. Neste trabalho, de forma a ser coerente com a norma, a geração das métricas

de risco seguiu o modelo apresentado pela ISO/IEC 27004 e que pode ser consultado no Anexo 1 deste trabalho.

Na ISO/IEC 27001, está estabelecido que o desempenho do sistema de gestão deve ser monitorizado. Contudo, como isto deve ser implementado não está descrito no documento. Dessa forma para aliviar esta falta de instruções, a norma ISO/IEC 27004 foi publicada em 2009, sendo a que ainda é aplicável nos dias de hoje, como ferramenta para a medição do desempenho da segurança da informação nas organizações. Esta norma exige que essas medições sejam comparáveis e reproduzíveis para que sejam capazes de serem usadas nas medições seguintes [13].

Como referido na ISO/IEC 27004, um método de medição pode usar objetos de medição e atributos que pode vir de uma grande variedade de fontes. Para este trabalho interessa-nos os objetos e consequentes atributos que surgem de uma apreciação do risco.

De acordo com [23], uma vez que um programa de medição de segurança da informação esteja implementado com sucesso, este pode:

- Demonstrar a conformidade da organização com requisitos legais e regulamentares e/ou obrigações contratuais;
- Suportar a identificação de questões de segurança da informação não detetadas anteriormente ou desconhecidas;
- Satisfazer as necessidades de reportar à gestão, provando trabalho através de medições para as atividades correntes;
- Ser usada como entrada para um processo de gestão do risco da segurança da informação, auditorias internas ao SGSI e revisões da administração.

2.3.4 ISO 27005 – Information technology – Security techniques – Information security management – Measurement

A norma fornece diretrizes para a gestão do risco na segurança da informação (em inglês, *Information Security Risk Management* - *ISRM*) numa organização, suportando especificamente os requisitos de um SGSI definido pela norma ISO/IEC 27001.

A norma ISO/IEC 27005 é aplicável em todos os tipos de organização. Ela não fornece ou recomenda uma metodologia específica. Isso irá depender de um grande número de fatores, tais como o objetivo e campo de aplicação atual do SGSI e do setor da organização.

Considerando a Figura 2, neste trabalho foi considerado o estabelecimento do contexto, a análise do risco, que inclui a identificação do risco, a estimação do risco e a apreciação do risco, que inclui a análise do risco, referida anteriormente, e a avaliação do risco. Seguindo o processo encontra-se o primeiro ponto de decisão que questiona se a apreciação do risco é satisfatória, neste ponto o trabalho foi desenvolvido considerando-se que a apreciação foi satisfatória. A partir deste ponto, e seguindo a resposta positiva, passou-se para o tratamento do risco e onde se distanciou do processo apresentado, pois foi somente realizada uma recomendação de controlos capazes de mitigar os riscos.

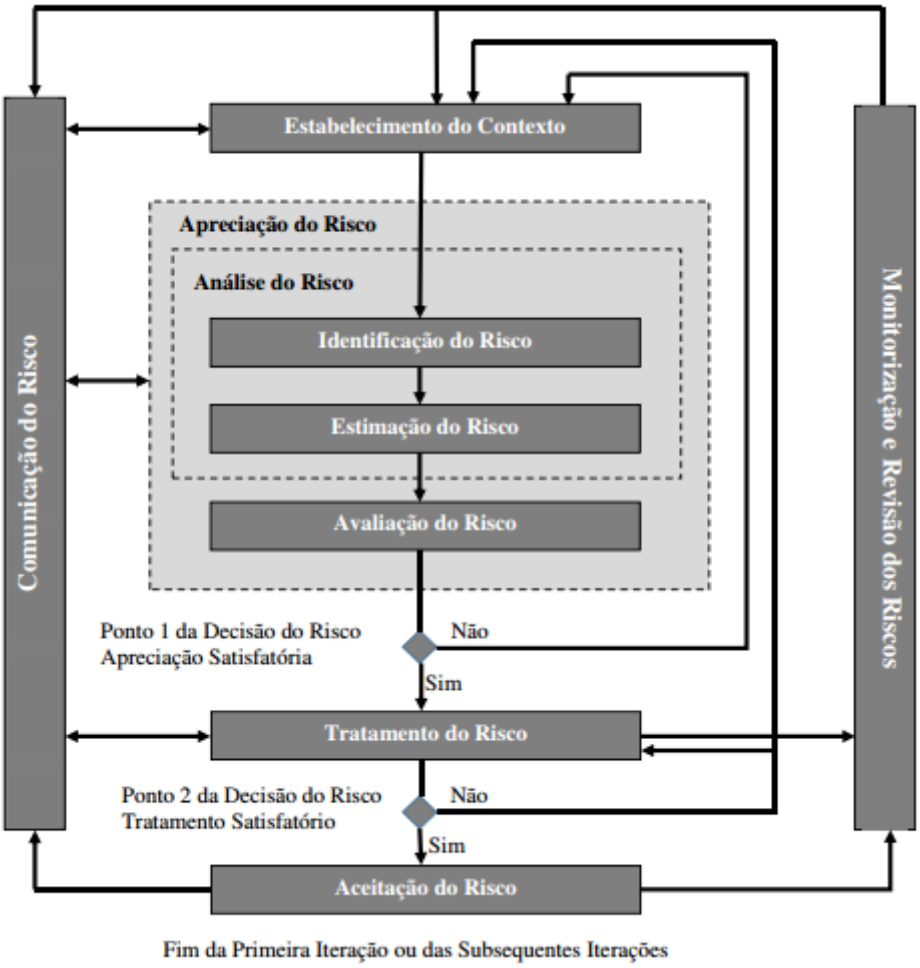


Figura 2. Processo de gestão do risco apresentado pela ISO/IEC 27005

2.4 Sistema de Gestão de Segurança da Informação (SGSI)

Toda esta família de normas define um SGSI bem estruturado. Um SGSI deve ser implementado por especialistas, pessoas que entendem os riscos e compreendem como os recursos da organização devem ser usados para mitigar esses riscos e como novos controlos podem ser implementados na organização sem que sejam necessárias grandes reformas.

Um exemplo de um bom SGSI deve incluir regras e responsabilidades bem definidas que devem estar descritas dentro da política do SGSI. Esse documento deve também prescrever como e onde as relações entre os vários componentes do sistema e ambiente da organização se interligam de forma a compreender a extensão que um dado controlo implementado ou perceber que consequências ou alterações na arquitetura do sistema uma implementação de um controlo pode causar. Um SGSI efetivo deve ter um claro e inequívoco suporte da administração assim como uma clara e demonstrável gestão do risco – com a habilidade de ligar riscos identificados e planos de tratamento de riscos, incluindo o registo de ações preventivas e corretivas.

As fundações sólidas de um SGSI bem construído devem ser também completamente documentadas. Deve-se experimentar e testar procedimentos de gestão de incidentes, procedimentos de auditorias internas e registo de atividades e acima de tudo ter uma estratégia clara de como as medições devem ser usadas para medir a eficiência dos controlos que fazem parte do processo de segurança da informação [13]. A segurança que pode ser atingida através de meios técnicos é limitada e deve ser suportada por gestão e procedimentos apropriados [22].

A ISO/IEC 27001, em 2005, apresentava o ciclo de implementação de um SGSI, conhecido como PDCA, Figura 3. Este conceito foi primeiramente desenvolvido para a área da gestão da qualidade, mas devido à eficácia dos processos e alcance de metas quando este era implementado, o conceito foi também adotado para a área da GSI.

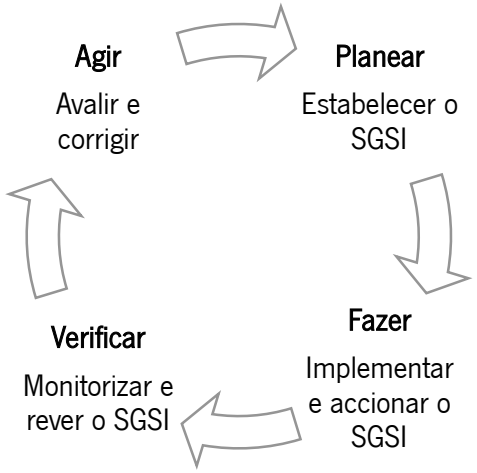


Figura 3. Ciclo de implementação de um SGSI apresentado pela ISO/IEC 27001: 2005

A primeira fase **Planear (*Plan)*** é responsável pela definição de metas, objetivos, análise de problemas, causas e elaboração de planos de ação. A fase seguinte é **Fazer (*Do)***, que

é o elemento responsável por implementar as mudanças recomendadas, através de treino e execução de planos de ação. De seguida, a fase **Verificar (*Check*)**, consiste em recolher informação e validar as medições exigidas, ou seja, verificação dos resultados. Por último, temos a fase **Agir (*Act*)**, na qual se realizam análises comparativas dessas medições, de forma a existir a padronização de resultados e o tratamento de desvios.

Com um estudo rápido à ISO/IEC 27001: 2013 pode-se concluir erradamente que este ciclo deixou de fazer parte da norma e pode dessa forma não ser considerado como uma ferramenta a utilizar na implementação de um SGSI. Mas esta ideia não está correta, citando [24], o ciclo PDCA não foi excluído, antes pelo contrário requer-se que "todas as normas ISO estruturem as suas cláusulas principais em torno deste ciclo". Este mesmo artigo identifica o reconhecimento do ciclo PDCA nas seguintes cláusulas:

- **Planear**: cláusula 4 (Contexto da organização), cláusula 5 (Liderança), cláusula 6 (Planeamento) e cláusula 7 (Apoio);
- **Fazer**: cláusula 8 (Operações);
- **Verificar**: cláusula 9 (Avaliação do desempenho);
- **Agir**: cláusula 10 (Melhoria).

2.5 Métricas de Segurança da Informação

Na era atual da tecnologia de informação, há uma necessidade crescente de soluções de segurança: sistemas de informação são mais vulneráveis por causa da complexidade crescente e da interligação de dispositivos e redes inseguros. Mesmo que aproximações adequadas de segurança possam ser encontradas, o nível resultante de segurança muitas vezes permanece desconhecido. Nesse sentido e citando [25], "as métricas fornecem introspeção, melhoram a visibilidade e a responsabilidade, e podem revelar a postura da segurança da informação completa da organização".

Elas podem ser métricas que mostram o verdadeiro risco a que as organizações estão expostas e sobre os quais tem de se tomar alguma decisão e outras podem surgir como métricas que avaliam a eficiência dos controlos já implementados.

De acordo com [10], não só a administração precisa de estabelecer a direção que a segurança deve seguir na organização, como também de estabelecer uma forma de ser capaz de ver e compreender como as suas diretivas estão ou não a ser atendidas.

"O objetivo primário das métricas é quantificar informação para facilitar a compreensão" [15]. Se investir em segurança não faz parte de uma estratégia coesiva e coordenada, esses investimentos tendem a ser mais um desperdício que um benefício [8].

Com o aumento da fraude de identidades, custos de TI ascendentes e escândalos corporativos frequentes, as entidades reguladoras estão a começar a fazer perguntas incómodas sobre como os CIO, os CEO e corpos de gestão estão a gerir o risco e portanto, a eficiência das suas estratégias de mitigação dos riscos, incluindo a segurança da informação [13].

As métricas, de acordo com [9], são uma ferramenta efetiva para os gestores de segurança da informação discernirem a eficiência de vários componentes nos seus programas de segurança, a segurança de um sistema específico, produto ou processo, e a habilidade do corpo profissional ou departamentos dentro da organização endereçarem as questões de segurança pelas quais são responsáveis. As métricas podem também ajudar a identificar o nível de risco, em não tomar determinada ação e dessa forma fornecer diretrizes para priorizar ações corretivas. Adicionalmente, elas podem ser usadas para aumentar o nível de consciencialização sobre a segurança da informação dentro da organização. Finalmente, com o conhecimento ganho através das métricas, os gestores de segurança podem responder de forma exata às perguntas difíceis dos seus executivos, tais como:

- A organização está mais segura hoje que ontem?
- Como podemos comparar a organização com outras a respeito disso?
- A organização está segura o suficiente?

Requer tempo e uma aproximação honesta e realística para concordar quais são as medições que podem ser efetivas para a organização e, mais significativamente, como é que se pretende medir a eficiência de forma a garantir que os resultados são reproduzíveis e comparáveis [15].

Unidades de medição para uma métrica podem incluir contas, frequências, percentagens assim como valores físicos. Uma métrica é diferente de uma medição pois ela é recolhida ao longo do tempo e é utilizada para comparar com valores anteriores. Esses valores podem ser recolhidos e depois comparados com o valor desejado para o sistema que se quer controlar. É essa habilidade de controlar um processo que faz das métricas uma ferramenta valiosa para as operações de TI sobre a segurança da informação [3]. Uma

organização pode ter centenas ou mesmo milhares de processos de negócio, mas deve-se focar só naqueles onde a sua perda resultaria num impacto maior para a organização.

Tendo em atenção o artigo [26], é necessário garantir que os gestores na realidade prestem atenção às métricas que serão desenvolvidas. O que é que o autor defende é o seguinte:

- É necessário que a organização reconheça a ligação entre as métricas, que a ela pertencem, e o sucesso do negócio. As informações apresentadas têm de ser do interesse das pessoas a quem a informação vai ser apresentada, e não só do interesse do gestor que gerou as métricas. Deve-se também usar termos que eles entendem e não cair no erro de usar linguagem técnica;
- Necessidade de as métricas criadas levar a ações e decisões. É necessário ter a perceção se as métricas criadas irão adicionar valor à organização;
- Várias perguntas podem surgir durante o programa de métricas, e a todas elas os gestores de segurança têm de ser capazes de dar resposta: se a métrica aumenta, a confiança na organização é maior? Se a métrica descer, alguma ação imediata tem de ser tomada e há alguém na organização que se importa? Se for necessário mudar a métrica, é possível?
- Se se quer ver resultados resultantes do modelo de métricas, tem que se ter a administração do topo empenhada em que se monitorize as métricas e se tome uma ação quando aparece um problema. Se não houver consequências para um desempenho pobre, então este é aceite e dessa forma nada irá mudar, deixando de existir um motivo para a existência de um modelo de métricas;
- Ter a certeza que as métricas são razoáveis, atingíveis e suportadas pelas metas da organização;
- As métricas devem conduzir a um tipo certo de melhoramento. Um dos riscos nas métricas é criar uma ferramenta que tanto conduza a consequências não intencionadas ou permite que o corpo profissional ‘brinque’ com o sistema. Para proteger a organização, deve-se fazer revisões periódicas aos comportamentos que as métricas estão a gerar e ajustá-los se necessário.

De acordo com [27], métricas efetivas devem conduzir a ações, decisões ou discussões importantes na organização. De acordo com [28], [29] e [30], mesmo que a maioria das organizações dependam de métricas para a melhoria operacional em TI, mais de metade dos profissionais de TI parecem estar preocupados com a sua capacidade de usar métricas para comunicar eficazmente com os executivos seniores sobre a segurança da informação.

De acordo com [31], as métricas de segurança são medições objetivas da eficácia de processos e/ou controlos de segurança. O propósito de ter métricas de segurança, é ter a noção que o que medimos deve responder a questões que são colocadas antes da medição.

As métricas têm de medir o que importa, e isso que importa deve ajudar a organização a ser proactiva em vez de reativa. Colocando de outra forma, métricas úteis contam o que se está a fazer relativamente àquilo que já estava a ser feito anteriormente.

Começar pequeno e despender tempo na formulação do problema, pois é nesta fase que a maior parte das organizações falham. Elas saltam diretamente para a geração das métricas sem considerarem as questões a que elas querem responder realmente.

Informação disponível impulsiona a geração de métricas. Deve-se começar com informação que está disponível e crescer-se a partir daí, de forma que a organização consiga controlar o processo que esta a implementar. Mas não se deve cair no erro de acreditar que as únicas questões a que se pode responder são aquelas que são suportadas pela informação disponível. As questões devem evoluir conforme a necessidade encontrada e a partir desse ponto recolher informação de forma adequada.

Sobre as métricas que devem ser usadas dentro da organização, deve-se perceber que a métrica deve contribuir de alguma forma para os objetivos de segurança da informação, os quais a organização precisa de preencher. A habilidade de aplicar uma métrica de segurança é dependente das capacidades individuais da organização. As capacidades de segurança podem representar a conexão entre objetivos de segurança da informação e métricas para a gestão do risco dessa segurança. De forma a determinar a métrica mais adequada para a geração da métrica para um dado objetivo, é necessário avaliar as métricas possíveis com respeito às capacidades dadas [12].

Tendo tudo isto em consideração as métricas podem servir para:

- Mostrar melhoras contínuas;
- Mostrar conformidade com normas, leis, regulamentos;
- Justificar qualquer despesa futura validando assim decisões tomadas a nível de orçamento;
- Identificar onde os controlos implementados não estão a ser eficazes a atingir os seus objetivos, isso ajuda a estabelecer direções para atividades futuras;
- Fornecer confiança às partes interessadas da organização e partes terceiras que os controlos implementados estão a proteger a informação.

2.8 Revisão de Trabalhos em Métricas de Segurança da Informação

Apresentamos nesta secção as principais fontes de suporte teórico e prático desta tese de mestrado. Pretende-se integrar uma visão académica com uma visão mais pragmática, sendo que essa integração é mais adequada à realidade das organizações no setor da saúde, dos seus gestores e responsáveis pelo SI, possibilitando assim perceber o ponto de situação na área das métricas para a gestão do risco em segurança da informação.

Um princípio que é amplamente aceite nos mais variados setores de atuação das organizações, é que uma atividade não pode ser bem gerida se não conseguir ser medida e desta forma, métricas de segurança da informação oferecem trabalho como campo de investigação, possibilitando consequentemente o estudo de métricas para a gestão do risco em segurança da informação. Sendo que as métricas procuram auxiliar as tomadas de decisão, várias revisões de trabalhos e normas na área têm sido analisadas e revistas possibilitando assim que os processos de segurança de informação tenham ganho disciplina e rigor [32]. A importância de assegurar a segurança dos ativos de informação tem-se tornado mais crítica a cada ano [12].

Aquando da iniciação do trabalho e sabendo que a primeira etapa seria uma apreciação do risco, foi consultado o Engenheiro Carlos Fernandes, auditor interno de segurança da informação na DigitalSign, o qual se mostrou disponível em explicar a metodologia usada pela empresa, a nível da análise do risco utilizando a norma ISO/IEC 31000 [33]. Esta visão foi importante para saber como se faz uma auditoria interna e perceber melhor o conjunto de normas que foi estudado de seguida.

Tendo sido escolhida a família de normas ISO/IEC 27000, efetuou-se a análise da ISO/IEC 27001 para o estudo dos requisitos necessários ao desenvolvimento de um SI e analisou-se a ISO/IEC 27002 e a ISO/IEC 27799 como complemento à ISO/IEC 27001. Estas duas normas serviram para perceber melhor cada um dos controlos e como eles deviam ser implementados. Estudou-se também a ISO/IEC 27005 de forma a estudar o modelo de apreciação do risco proposto por esta e por fim a ISO/IEC 27004 para conhecer e fazer uso do método proposto por esta norma, sendo esta aplicada na organização em estudo, no contexto do desenvolvimento de métricas de risco de segurança de informação.

A norma ISO/IEC 27004, inclui uma descrição geral de um processo para a geração e uso de métricas de segurança da informação. Contudo, não está claro como esta norma pode ser introduzida nas organizações [20] e é neste ponto que este caso de estudo pretende

contribuir de forma mais explícita, pois o principal objetivo é mostrar a implementação desta norma na prática.

Foram considerados e analisados outros normativos, entre eles o NIST SP 800-30, revisão 1 [34], sendo este um guia para conduzir avaliações do risco e o NIST SP 800-55 revisão 1 [35] como guia para a medição do desempenho para a segurança da informação. A análise destes normativos permitiu perceber qual a família de normas que seria escolhida. Fazendo menção ao artigo [36], a norma NIST SP 800-30 destina-se em grande parte a uma apreciação do risco técnica, não sendo uma ferramenta útil para realizar apreciações do risco organizacionais. Esta norma difere primeiramente da ISO/IEC 27005 pois considera somente a caraterização do sistema (fronteiras, funções, criticidade e sensibilidade dos dados e do sistema), não sendo necessário dessa forma ter uma tabela com o levantamento dos ativos. A segunda grande diferença, e que foi também considerada na escolha da família de normas ISO/IEC 27000, foi a consideração das vulnerabilidades antes de ser feita a análise aos controlos existentes. A realização desta ação não permite considerar os riscos que esses controlos já estão a mitigar, fazendo dessa forma que se considerem riscos que não deveriam ser tidos em conta. A ISO/IEC 27005 possui assim uma visão mais realista, pois no perfil das vulnerabilidades considera os controlos implementados à posteriori na organização.

De acordo com [9] parece que a disciplina das métricas de risco é ainda um pouco imatura e entendida de diferentes maneiras. As métricas de segurança são uma área da segurança de computadores que tem recebido bastante atenção ultimamente. Este não é um tópico novo, mas um que recebe um interesse focado esporadicamente. Muito do que tem sido escrito sobre métricas de segurança é em termos de definição, tentativa de ajudar a fornecer orientações para definir uma métrica de segurança e especificar critérios que de alguma forma devem ser atingidos. Contudo, relativamente pouco tem sido demonstrado a nível das métricas atuais que se possam ter provado úteis na prática [37].

Alguns autores defendem que programas de segurança da informação que são menos maduros precisam de desenvolver as suas metas e os seus objetivos antes de serem capazes de aplicar um programa de métricas [25]. Este caso de estudo pretende mostrar o contrário, mesmo não tendo um programa bem definido é possível fazer uso de um conjunto de métricas que possam ajudar na tomada de decisões quanto à implementação de controlos, e assim também contribuir para a maturação do programa de segurança da informação que esteja implementado ou se pretenda implementar.

Muitas organizações já têm alguma ferramenta implementada que permite servir como evidência de bons controlos de segurança já implementados. Mas quando se começa a explorar o quê, como e o porquê desses controlos terem sido selecionados e como estão a ser agora monitorizados, verifica-se que esses processos não estão assim tão bem construídos e de longe, devidamente documentados [13].

Muitos processos usam métricas, um dos mais proeminentes e amplamente conhecido é o chamado Six-Sigma [4]. O Six-Sigma é uma abordagem quantitativa que permite melhorar a eficiência e eficácia de uma organização e é uma metodologia de melhoria de qualidade mais popular na história [38]. Mas existem várias outras ferramentas, que podem ser utilizadas para quantificar a eficiência dos controlos de segurança numa organização. Essas ferramentas normalmente dizem-nos como devem ser implementadas de forma a monitorizar os sistemas e dessa forma obter informações sobre os processos de segurança. As quatro ferramentas mais populares são os seguintes [5]:

- COBIT (*Control Objectives for Information Technology)*: fornece um conjunto de boas práticas as quais são úteis para as organizações implementarem governação e controlo das TI;
- ISO/IEC 27002: fornece recomendações de boas práticas na gestão da segurança da informação em ordem a iniciar, implementar e manter um SGSI. Os controlos e os objetivos da segurança da informação estão descritos em cada seção e para cada um dos controlos de segurança é fornecida orientação para a sua implementação;
- ITIL (*Information Technology Infrastructure Library):* esta ferramenta contem um conjunto de práticas para o *Information Technology Services Management* (ITSM). Esta é muito mais geral que as ferramentas anteriores, ela não se foca só em tópicos de segurança. A gestão da segurança com ITIL descreve como a segurança da informação deve encaixar-se na gestão de uma organização e esta é baseada na ISO/IEC 27002;
- A série de normas NIST SP 800: este conjunto de documentos é apresentado pelo Instituto Nacional de Normas e Tecnologia dos Estados Unidos. O documento SP 800-18 e o SP 800-80 especifica 17 famílias de controlos de segurança de alto nível. O SP 800-30 introduz orientações sobre a gestão do risco nos sistemas de tecnologia de informação e norma SP 800-55 é um guia para a geração de métricas de segurança [12].

De acordo com [25], as práticas correntes da apreciação da segurança foca-se em querer medir a eficácia do programa de segurança, auditoria e avaliação de componentes de sistemas de informação individuais, como redes e *software*. Há discrepâncias na forma como é dado significado à segurança e esta é quantificada em várias outras abordagens. Estas discrepâncias afetam a sua adoção como programas que derivam resultados de medição confiáveis.

Através do artigo [39], podemos analisar o tipo de métricas que existem atualmente:

- **Métricas de risco da segurança**: estas apresentam-se como o instrumento para a avaliação do sistema de segurança, medindo o tamanho da incerteza que as consequências para o negócio da organização irão aparecer por causa das ameaças e fraquezas do sistema de segurança;
- **Métricas para modelos de maturidade**: estas avaliam as características de segurança de objetivos e campos de aplicação mais amplos. Elas estão mais orientadas para medir o suporte da administração e avaliação dos processos bem-sucedidos;
- **Métricas para avaliar metas e indicadores de desempenho**: são métricas para monitorizar indicadores de risco, para monitorizar o grau de implementação do programa de segurança, para monitorizar o grau da realização das metas de segurança e métricas usadas para avaliar os aspetos dos processos de negócio em relação às melhores práticas dentro da área de intervenção da organização;
- **Métricas para calcular o retorno sobre o investimento na segurança da informação**: estas fazem parte de um grupo especial de métricas que pretendem apresentar a rentabilidade do capital investido na segurança.

Há autores que defendem que é necessário assegurar que o programa de segurança esteja completo antes de se aprofundar no desenvolvimento de métricas para evitar o lado mau das métricas. Outros autores defendem que as organizações frequentemente constroem programas de métricas da informação muito básicos que depois vão evoluindo, resultando em métricas suportadas pelos produtos de segurança disponíveis, em vez de se focarem naquelas métricas que são significantes para o negócio.

Hoje nesta área, muitos trabalhos estão neste momento publicados: NIST SP 800-55 (revisão 1) [35], ISO/IEC 27004 [23], relatório de métricas realizado pelo CIS [40], conjunto de documentos produzidos pelo *SANS Institute* que exploram o mundo das

métricas de segurança como é o caso dos artigos [4], [9] e [41] e ainda um relatório produzido pela ENISA, que representa uma tentativa de criar uma única fonte técnica de informação em métricas de resiliência, as taxonomias e as questões em aberto na área.

O mundo dos trabalhos e publicações sobre as métricas de segurança de informação teve a sua primeira grande publicação em 2003 quando surgiu o documento do NIST SP 800-55 Guia de Métricas de Segurança para Sistemas de Tecnologia de Informação (título original NIST SP 800-55 *Security Metrics Guide for Information Technology Systems*). De acordo com [16], "o documento fornece orientações, através do uso de métricas, identifica a adequação dos controlos de segurança implementados, políticas e procedimentos. Fornece uma abordagem para ajudar a gestão a decidir onde investir em proteção de segurança adicional ou a identificar e avaliar controlos não produtivos." Foi a primeira grande publicação sobre métricas de segurança, tendo sido a primeira a 1) identificar a necessidade de as métricas de segurança se alinharem com os objetivos de negócio e da cultura organizacional, 2) identificar a necessidade de agregar métricas para acomodar diferentes vistas hierárquicas dentro da organização e também a 3) apresentar a ideia de ponderação de algumas métricas sobre outras. A partir da apresentação dessas três necessidades deixou de se ver as métricas de segurança como um conceito de que estas podem ser aplicadas a todas as organizações da mesma forma. Esta norma tem fornecido aos profissionais de segurança e tecnologia de informação um processo para desenvolver, selecionar e implementar medições de desempenho para facilitar a tomada de decisões, melhorar o desempenho e aumentar a transparência. Ela descreve como é que uma organização pode usar o seu sistema de segurança e os controlos do programa de segurança para conseguir atingir a sua missão.

Nesse mesmo ano, a ferramenta COBIT, criada pela ISACA, apareceu como ferramenta de governação de TI que mudou a forma como os profissionais de TI trabalhavam, pois esta ajudou a compreender as necessidades de governação de TI e a garantir a integridade dos sistemas de informação e da própria informação. Com a vinculação entre as práticas de tecnologia informática e as práticas de controlo, o COBIT consolida e harmoniza normas proeminentes de fontes globais num recurso importante para a administração, profissionais de controlo e auditores. O objetivo do COBIT é proporcionar à administração e aos proprietários dos processos de negócio um controlo de governação de TI para ajudar a entender e gerir os riscos associados a esta e ajuda a preencher as lacunas entre os riscos de negócio, necessidades de controlo e aspetos técnicos. Em 2012

foi publicada versão seguida atualmente, sendo esta o COBIT 5. Esta versão documenta os 5 princípios do COBIT 5 e define os sete habilitadores que apoiam a composição do modelo. O COBIT permite às organizações maximizar o valor e minimizar o risco relacionado com a informação. Este é um modelo abrangente dos princípios globalmente aceites, das práticas e das ferramentas analíticas e que podem ajudar qualquer organização a resolver efetivamente problemas críticos dos negócios relacionados com a governação e a gestão da informação e tecnologia.

No ano seguinte em 2004, surgiu o grupo chamado *Security Metrics Consortium*, sendo que a missão deste grupo era "definir métricas de risco de segurança quantitativas padronizadas para a indústria e adoção dos vendedores e fornecedores" [42]. Tinha também como objetivos "criar um painel de segurança definitivo e expandir as métricas de risco de segurança para incluir conformidade com políticas". Esta era a missão e algum dos objetivos, mas o grupo nunca chegou a atingir o pretendido aquando da sua criação e por conseguinte, não conseguiu contribuir para a área das métricas de segurança. Nesse mesmo ano foi publicado relatório realizado por *Corporate Governence Task Force Report*, intitulando-se *Information Security Governance*. Este relatório adicionou algumas ideias novas ao conceito de métricas de segurança. Primeiro as métricas deviam estar alinhadas com o desenvolvimento do sistema e o seu ciclo operacional de vida do mesmo. O esforço foi colocado nas operações e na fase de manutenção e considerava também que as métricas de segurança deviam ser escaláveis. Pode-se afirmar que esta foi outra tentativa de se distanciar da noção de que um conjunto de métricas podia ser aplicado a qualquer organização independente do setor de atuação. Um terceiro ponto que é promovido no relatório, é a ideia que a segurança é uma responsabilidade empresarial e corporativa e não uma responsabilidade única do departamento de TI. Por fim sublinha, que as métricas de segurança devem considerar pessoas e processos, e não só tecnologia [42].

No ano de 2005 surgiu a ISO/IEC 27001 *Information technology – Security techniques – Information security management systems – Requirements*, substituindo a norma BS 7799-2, que era essencialmente um código de boas prática. Nesta primeira versão da norma é de forma evidente usado o modelo PDCA para estruturar os processos e refletir os princípios definidos nas orientações da OECD. Esta norma foi revista e publicada novamente em 2013, sendo a esta a versão que é usada hoje em dia. Tendo em consideração a versão de 2005, esta versão coloca mais enfase em medir e avaliar se as

metas do SGSI da organização estão a ser atingidas. Uma atenção adicional foi prestada ao contexto da segurança da informação dentro da organização. Citando [43], o objetivo dela é fornecer requisitos para estabelecer, implementar, manter e continuamente melhorar um SGSI. Afirmando ainda que o desenho e implementação de um SGSI é influenciado pelas necessidades e objetivos da organização, requisitos de segurança, processos organizacionais usados e tamanho e estrutura da organização.

No mesmo ano que foi lançada a ISO/IEC 27001, foi também publicada a ISO/IEC 270002 *Information technology -- Security techniques -- Code of practice for information security management.* Esta foi originalmente publicada como a renomeação da existente norma ISO/IEC 17799. Sendo um código de prática para a segurança da informação, ela basicamente esboça centenas de potenciais controlos e mecanismos de controlo, os quais podem ser implementados, em teoria. Ela estabelece orientações e princípios gerais para iniciar, implementar, manter e melhorar a GSI na organização. Os objetivos esboçados fornecem diretrizes gerais sobre as metas comumente aceites da GSI. Esta norma contem as melhores práticas de objetivos de controlo e controlos. Os controlos listados na norma destinam-se a endereçar os requerimentos específicos identificados via uma apreciação do risco formal. Esta norma destina-se a ser uma base comum e uma orientação prática para desenvolver normas de segurança organizacionais e práticas de gestão da segurança eficazes e ajudar a construir confidencialidade dentro das atividades internas organizacionais. Esta norma foi também revista em 2013, sendo que a versão revista tem 144 controlos, em oposição aos 133 documentados na versão de 2005. Contudo, de forma a adicionar granularidade, estes são apresentados em 14 seções, em vez das 11 originais. Esta norma foi desenvolvida de forma a poder ser usada pelas organizações para selecionar controlos dentro do processo de implementação de um SGSI baseado na ISO/IEC 27001 e desenvolver as suas próprias orientações de GSI.

Também nesse ano foi publicado o relatório *Report of Best Practices and Metrics Teams*, sendo este realizado pelo *Corporate Information Security Working Group.* Este relatório promovia o uso da utilização das métricas de segurança para identificar riscos, estabelecer limites de desempenho aceitáveis para a tecnologia e os processos relacionados com a segurança e medir as estratégias de implementação, políticas e controlos para mitigar os riscos identificados na organização [44].

Em 2008 surgiram outras duas publicações importantes para a área das métricas, uma delas foi o documento NIST SP 800-55 entitulado *Performance Measurement Guide for*

Information Security sendo este a revisão da versão de 2003 do documento NIST SP 800-55. Em relação ao anterior este fornece orientações adicionais ao nível de programas para medir o desempenho da segurança da informação em suportar as métricas e estratégias organizacionais. Ele também alinha a medição do desempenho com os controlos de segurança no documento NIST SP 800-53 – *Recommended Security Controls for Federal Information Systems*. Foi também publicada a norma ISO/IEC 27799 *Health informatics -- Information security management in health using ISO/IEC 27002*. Esta norma define orientações para suportar a interpretação e implementação da ISO/IEC 27002 no setor da informática na saúde e deve sempre acompanhar a ISO/IEC 27002 neste setor. Esta especifica um conjunto de controlos detalhados para gerir a segurança da informação de saúde e dessa forma fornece as melhores orientações práticas para este setor. O que é esperado, é que as organizações de saúde e organizações terceiras a estas, mas que também armazenem informação de saúde, sejam capazes de assegurar um nível mínimo de segurança necessário. Esse nível deve estar de acordo com as circunstâncias organizacionais e será este que irá ser capaz de manter a CID da informação pessoal de saúde dos pacientes. A norma aplica-se à informação do setor da saúde em todos os aspetos, independentemente da forma como a informação está armazenada (palavras e números, gravação de sons, vídeo ou imagens médicas), da forma que será usada para a armazenar (impressa, escrita em papel ou armazenada eletronicamente) e da forma que será usada para a transmitir (por mão, via fax ou através das redes de computadores), toda esta informação deve ser sempre protegida adequadamente. Esta norma foi revista e publicada em julho de 2016. Esta fornece orientação na implementação dos controlos descritos na ISO/IEC 27002 para a área da saúde e complementa-os se necessário, para que dessa forma eles possam ser efetivamente usados para gerir a segurança da informação de saúde. Em conjunto com a ISO/IEC 27002, esta norma define o que é exigido em termos de segurança de informação no setor da saúde, mas não define como eles devem ser atingidos.

Em 2009 a publicação central a esta tese de mestrado, sendo esta a ISO/IEC 27004 *Information technology – Security techniques – Information security management – Measurement* foi publicada. A norma oferece orientação no desenvolvimento e uso de medidas e medições para a avaliação da eficácia de um SGSI e dos seus controlos, como especificado na ISO/IEC 27001. De acordo com [23] esta pretende ajudar as organizações

a estabelecerem a eficácia da implementação dos seus SGSI, a fazerem comparações entre sistemas e focarem o desempenho dentro do ciclo PDCA.

Foi neste mesmo ano que foi publicado também um relatório do NIST, intitulado NISTIR 7564 *Directions in Security Metrics Research*. Segundo [37], "a área das métricas de segurança tem-se demonstrado com problemas difíceis e multifacetados para os investigadores. Uma resolução rápida não é esperada e a probabilidade é que nem todos os aspetos desses problemas sejam resolvidos. Além disso, apenas alguns desses aspetos que têm solução podem ser capazes de ser feitos de forma satisfatória, atendendo às expectativas de repetibilidade, reprodutibilidade, relevância, oportunidade e custo. Vários fatores impedem o progresso nas áreas das métricas de segurança:

- A falta de bons estimadores da segurança do sistema;
- A confiança enraizada em entradas subjetivas, humanas e qualitativas;
- Os meios demorados e evasivos comumente usados para obter as medições;
- A falta de compreensão e discernimento sobre a composição dos mecanismos de segurança.

O documento propõe várias linhas de investigação que podem ser endereçadas a estes fatores e podem ajudar a fazer progressos no estado da arte em métricas de segurança. As seguintes áreas de investigação foram identificadas:

- Modelos formais de métricas e medições de segurança;
- Recolha e análise do histórico de informação;
- Técnicas de apreciação da inteligência artificial;
- Métodos de medição realmente praticáveis;
- Componentes intrinsecamente mensuráveis."

No ano seguinte, em 2010, o relatório *The CIS Security Metrics* [45] contribui para a área fornecendo um conjunto de métricas de segurança relacionadas com a gestão do risco envolvendo funções de negócio. A categorização feita incluiu métricas de Gestão de Incidentes, Gestão de Vulnerabilidades, Gestão de *Patches*, Segurança das Aplicações, Gestão de Configurações e ainda métricas financeiras.

Em 2011, surgiram mais dois relatórios na área das métricas de segurança, sendo um deles o *Information Security Metrics: State of Art* onde ficou demonstrado que "embora muito progresso tem sido feito na área buscando o estabelecimento de um entendimento comum, como por exemplo o porquê da importância de medição da eficácia da segurança e o que

está envolvido, certos mal entendimentos e lacunas na metodologia e conhecimento entre as várias partes interessadas permanecem. Uma dificuldade percebida passa por traduzir métricas de camadas mais baixas em métricas de camadas mais altas. As aproximações ao desenvolvimento de métricas de topo podem, em teoria, serem usadas para derivar objetivos de medição de camadas mais baixas assim como estabelecer uma linha de comunicação para apresentar os resultados, mas não há num procedimento comumente aceite para se fazer isso. Possivelmente o maior desafio na medição da segurança (e dessa forma, na gestão de segurança em geral) é que os objetivos, capacidades e a mudança constante do ambiente e os controlos de segurança devem estar todos adequadamente alinhados. Embora seja possível expressar os objetivos numa forma quantitativa e clara e o estado de arte das ferramentas de medição tendem a se responsabilizar pela capacidade/maturidade do SGSI, elas não tratam o ambiente de forma formal ou normalizada (em vez disso, o contexto operacional é normalmente estabelecido por meios de gestão do risco). Uma vez que a eficácia e adequação definitiva dos controlos pode somente ser determinada de acordo com a visão do ambiente em que está inserida, o nível de formalidade da sua apreciação deve refletir o nível das métricas de eficácia de segurança." [46] O outro relatório foi produzido pela ENISA, intitulando-se *Measurement Frameworks and Metrics for Resilient Networks and Services: Technical Report* [47] Relatório produzido pela ENISA. Este relatório representa uma tentativa de criar uma fonte técnica única de informação sobre métricas de resiliência, taxonomias e questões em aberto. Ele sumariza o trabalho, tendo como foco principal a resiliência que tem sido feito nas áreas de segurança e na investigação das específicas taxonomias. Pretende-se que este se torne uma fonte de informação para a comunidade interessada em resiliência e medições, mas também motivar a iniciação de trabalhos mais profundos nesta matéria. Foi também neste ano que foi publicado a última versão da ferramenta ITIL, que é a ferramenta para a gestão de serviços de TI mundialmente mais adotado. As utilizações das melhores práticas contidas nesta ferramenta ajudam as organizações a atingirem seus objetivos de negócio utilizando adequadamente os serviços de TI. Ela introduziu um conjunto de processos estratégicos claramente definidos, incluindo a Gestão Estratégica para Serviços de TI e Gestão da Relação de Negócio.

A última publicação estudada foi publicada em 2015, sendo esta a *A Measurement Companion to the CIS Critical Security Control,* que foi produzida pelo CIS. De acordo com [40] pretende-se que os adotantes de métricas de segurança, possam usar esta

amostra de métricas como um ponto inicial para identificar informação chave que os possam ajudar a acompanhar o progresso da organização e encorajar o uso de automação para recolha de dados. Este identifica que há muitas coisas que podem ser medidas, mas não está claro quais dela vale a pena medir, de forma a adicionar valor às decisões de segurança. Identifica também que há poucas ideias absolutas em segurança, pelo que haverá sempre o desafio de fazer um julgamento sobre o valor de medição que é "bom o suficiente" em termos de gestão do risco. O relatório não pretende solucionar o problema de terminologia inconsistente que atravessa as indústrias, mas pelo menos se manterem consistentes dentro dos controlos de segurança críticos identificados pelo CIS.

O tema das métricas de segurança também tem sido muito explorado através de artigos em vários sites da área de sistemas de informação. temos exemplos de sites como www.csoonline.com, www.securitymetrics.com e www.computerworld.com.

Esta dissertação assenta num caso de estudo desenvolvido num centro hospitalar em Portugal. Este surgiu como forma de aprofundar a geração de métricas num ambiente hospitalar. Muitos dos trabalhos desenvolvidos nesta área passam por metodologias mais ou menos desenvolvidas e o que assim elas acarretam, trabalhos muito teóricos e pouco tendo em conta o ambiente em que as organizações estão inseridas, exemplos destes trabalhos encontram-se em [12], [25] e [39].

Já que os pesquisadores não têm muito controlo sobre o fenómeno que é a geração de métricas, o caso experimental vem trazer mais luz a este tema. Sendo importante estudar este tema dentro do contexto onde ele ocorre naturalmente. Como assim se depreende esta é uma estratégia de pesquisa que contém um método que abrange quer a apreciação do risco quer a geração de métricas de risco de segurança da informação em abordagens específicas de recolha e análise de dados.

Foi decidido fazer um caso de estudo analítico por se querer testar teorias. Isso permitirá compreender a geração de métricas fazendo uso da ISO/IEC 27004. Deste tipo de caso de estudo pretende-se construir ou desenvolver novas teorias que irão ser confrontadas com as teorias que já existem, proporcionando assim avanços do conhecimento.

É preciso que haja diferentes visões teóricas acerca do assunto estudado, pois serão a base para orientar as discussões sobre determinado fenômeno e constituem orientação para discussões sobre a aceitação ou não das alternativas encontradas. Para isso é preciso

possuir uma amostra de várias evidências e neste sentido é importante a existência de estudos práticos para reforçar esta área.

3 Metodologia

Sendo este um caso de estudo prático este é especialmente útil porque testa modelos teóricos, usando-os em situações reais. Basicamente, um caso de estudo é uma investigação aprofundada de uma situação particular ao invés de um levantamento estatístico. É o método usado para restringir um campo de investigação muito amplo num tópico facilmente investigável. Com este trabalho pretende-se restringir a área da segurança da informação e investigar o tópico específico das métricas de risco da segurança da informação e da sua geração. Ele não responde a uma pergunta completamente, mas dá indicações, permitindo uma maior elaboração e criação de uma hipótese sobre o tema das métricas de risco da segurança da informação, num contexto hospitalar.

Sendo o caso de estudo do tipo *research design* este é útil para testar se teorias cientificas e modelos trabalham verdadeiramente no mundo real. Pode-se criar ou falar de modelos de métricas para vários setores, fazer estudos teóricos, mas só mesmo desenvolvendo-o num ambiente organizacional é que vamos perceber se realmente isto pode ser realizado na organização e se realmente faz sentido.

Como este trabalho se baseia na série de normas da ISO/IEC 27000, usou-se a norma ISO/IEC 27005 como ferramenta a utilizar para a apreciação do risco e utilizou-se a norma ISO/IEC 27004 como ferramenta para a geração do modelo de métricas de segurança da informação.

Para o desenvolvimento do modelo de métricas foram consideradas quatro hipóteses, sendo que de 1 à 3 surgiram do estudo do artigo [18]:

1. A produção de um inventário de fontes de informação disponíveis e deixar que isso ditasse as métricas a serem geradas, por causa da informação disponível. Tem-se a certeza que as métricas podem ser geradas, porque de antemão já se sabe que a informação está disponível;
2. A consulta de materiais de referência em métricas de segurança e compilar uma lista de potenciais medições, e no final escolher aquelas que são mais facilmente alcançáveis dentro do ambiente da organização;
3. A condução de entrevistas com as partes interessadas da organização, aprender quais são as medições que são importantes para eles e desenvolver uma forma de recolher a informação necessária para a geração das métricas;

4. A condução de uma apreciação do risco e daí perceber quais são os controlos que se querem medir, prosseguindo de seguida com a geração das métricas de segurança da informação. A apreciação do risco ao centro hospitalar centra-se em 5 aplicações que fazem parte do núcleo funcional da organização;

Este trabalho enquadrou três destas hipóteses: primeiro foi realizada uma apreciação do risco para perceber quais os controlos mais importantes a medir, de seguida foi feita uma lista com a compilação das métricas de risco de segurança da informação relacionadas com a recomendação de controlos, para mitigar os riscos mais críticos e por fim, pegando na compilação das métricas realizou-se de seguida entrevistas com os administradores dos sistemas de informação do centro hospitalar de forma a perceber quais as métricas mais importantes para eles e aquelas que eram capazes, de neste momento se adaptarem melhor à organização e chamar mais a atenção da administração. Essas métricas foram também escolhidas de forma a mostrarem se a organização está ou não em conformidade com o RGPD.

Não se pretendeu fazer uma apreciação do risco ao sistema inteiro do centro hospitalar devido à grande dimensão do mesmo, e pelo fato de ser necessário desenvolver este trabalho dentro de um período de tempo restrito. Como participantes neste caso de estudo, que se desenvolveu com base em entrevistas, de salientar os vários administradores das aplicações em estudo e a participação do diretor dos sistemas de informação do centro hospitalar.

Através das entrevistas foi possível perceber a opinião do entrevistado sobre o assunto em questão e ter a perceção completa do ambiente, que pode ser considerado, como exemplo de qualquer outro centro hospitalar em Portugal.

3.1 Apreciação do Risco

Uma análise do risco é uma parte integral da prática de gestão e um elemento essencial de governação corporativa, sendo esta entendida como sendo o sistema de regras, práticas e processos pelos quais a organização é dirigida e controlada [47]. A prática de gestão, por seu lado, é constituída por atividades coordenadas para direcionar e controlar uma organização em relação ao risco.

De acordo com [48], o objetivo de uma apreciação do risco é identificar, priorizar e avaliar os riscos da segurança da informação aos quais os ativos da organização estão expostos para que dessa forma os controlos apropriados possam ser selecionados e implementados.

Apreciações do risco são uma fotografia em um determinado ponto do tempo e deve, por isso, ser repetidas em períodos de tempo regulares de forma a assegurar que as mudanças no ambiente técnico e de negócio são capturadas.

Sem a realização de apreciações do risco, uma organização não terá informação precisa sobre forças e fraquezas, sendo que sem conhecimento sobre as áreas de fraquezas poderá aumentar a probabilidade da ocorrência de incidentes de segurança [48].

Em prática, os administradores devem constantemente equilibrar a disponibilidade, a confidencialidade e a integridade. Esta tarefa envolve compromissos complexos, tipicamente específicos de cada sistema e organização, que requerem um balanço apropriado entre propriedades que não são inteiramente compatíveis umas com as outras [5].

Informação é um ativo chave para as organizações e reduzir o risco de comprometimento da informação é de prioridade elevada. O objetivo primário de qualquer organização é envolver a gestão de processos de negócio de forma a usar e manter sistemas de informação. O sistema de informação deve estar em conformidade com os objetivos de segurança, sendo estes a confidencialidade, integridade, autenticação, autorização e não repúdio de forma a garantir o funcionamento adequado dos processos de negócio [47]. Tendo o sistema a trabalhar, cada organização quer protegê-lo de sofrer qualquer dano – isto é o que a segurança da informação é, a proteção sistemática da informação contra qualquer perigo.

Uma apreciação do risco da segurança da informação é a base da proteção da informação, e faz parte da gestão do risco. Como uma gestão do risco exige uma avaliação precisa, como condição, a análise do risco é um aspeto indispensável da gestão da proteção da informação. A apreciação do risco, em particular, tem atraído um interesse maior e isso é evidente a partir do facto que ela é frequentemente usada como um ponto de início para eventos de segurança da informação.

A apreciação do risco é um componente importante na seleção e compilação de política de segurança da informação para a organização. Há muitos métodos disponíveis e cada um desses métodos foi gerado para um propósito particular usando abordagens diferentes, informação, nível de experiência/habilidades e parâmetros (de entrada e saída). É importante para uma organização, que está interessada em levar a cabo uma apreciação do risco, selecionar o método apropriado para resolver o seu propósito [47].

Numa primeira etapa foi realizada uma apreciação do risco, que consiste numa parte da implementação de um programa de gestão do risco. Para a elaboração desta etapa, foram levadas a cabo um conjunto de entrevistas ao conjunto de administradores responsáveis pelas aplicações em estudo. Este primeiro conjunto de entrevistas, composto pelas perguntas que podem ser consultadas na Tabela 18, teve como foco principal conhecer globalmente as aplicações que se iriam estudar. Qual a visão dos administradores quanto às aplicações que são da sua responsabilidade, o que eles entendem por risco, se reconhecem as vulnerabilidades dessas aplicações, e o que eles fazem no dia a dia para que estas fiquem mais seguras.

Depois deste primeiro conjunto de entrevistas, Tabela 18, fez-se uma análise aprofundada da ISO/IEC 27001, que contem os controlos a que um sistema de segurança da informação deve obedecer, e da ISO/IEC 27002 que elabora em mais detalhe cada um dos controlos. Esta análise foi realizada tendo em foco desenvolver um questionário, que servisse de base para o segundo conjunto de entrevistas, que está apresentado na Tabela 19. Este segundo conjunto de entrevistas serviu para que se fosse capaz de perceber em mais detalhe cada uma das aplicações e algumas das suas vulnerabilidades, que controlos estavam associados a elas e o que os administradores pretendiam que fosse desenvolvido no futuro.

Com estes dois conjuntos de entrevistas foi possível criar uma visão completa de cada aplicação. Essa visão inclui informação contida em cada aplicação em estudo, dispositivos físicos que sustentam a aplicação e os que são usados para aceder à mesma, o *software* usado pela aplicação, as pessoas que são responsáveis por ela e colaboradores que fazem uso da mesma, obtendo-se ainda informação dos controlos implementados atualmente relacionados com a aplicação. Isto serviu para que se avançasse para a execução da apreciação do risco que conteve as etapas abordadas nas subseções seguintes.

À medida que os riscos de segurança da informação e a eficácia dos controlos mudam dependendo de circunstâncias mutáveis, as organizações precisam de, [1]:

- Monitorizar e avaliar a eficácia dos controlos e procedimentos implementados;
- Identificar riscos emergentes que precisam de ser tratados;
- Selecionar, implementar e melhorar os controlos adequados como necessário.

Processos de análise do risco definem as variáveis críticas que, quando monitorizadas, mostram o nível de exposição ao risco e depois, determinam as métricas que irão medir a eficácia dos controlos [6].

Tomando conhecimento que a geração de métricas de segurança da informação deve ser derivada de necessidades de avaliação estabelecidas, esta análise foi realizada para identificar essas necessidades. A análise foi baseada em afirmações extraídas de entrevistas com o corpo profissional do centro hospitalar.

A análise resultou numa apreciação do risco com os seus vários resultados e esses mesmos resultados definiram as necessidades maiores que o centro hospitalar apresenta neste período de tempo definido em que foi realizado o trabalho.

3.1.1 Levantamento dos Ativos

Quando se iniciou o levantamento dos ativos, concluiu-se que os administradores que trabalham diretamente com as aplicações tinham alguma dificuldade em perceber o que realmente eram os ativos do sistema, considerando muitas vezes a parte mais tecnológica de cada aplicação.

Dessa forma as conversas levadas a cabo com cada administrador, correu de forma que o conceito de ativo fosse completamente entendido. Foi-lhes dado o seguinte conceito: "*Um ativo é qualquer coisa com valor para a organização"*. No seguimento das entrevistas e de forma a facilitar todo o processo os ativos foram divididos em quatro categorias:

- **Ativos de informação:** são os ativos que contêm informação preciosa para a organização. Cada peça de informação sobre a organização cai nesta categoria. Esta informação tem de ser recolhida, organizada e armazenada em várias formas. Como exemplos destes ativos de informação podemos encontrar, e considerando o descrito em [49]:
  - Bases de dados: informação sobre os pacientes, corpo profissional, finanças, etc.;
  - Ficheiros de dados: informação transacional com informação pormenorizada sobre cada evento;
  - Procedimentos operacionais e de suporte: estes foram desenvolvidos ao longo dos anos e fornecem instruções detalhadas sobre os procedimentos a se realizar nas várias atividades;

- Informação arquivada: informação antiga que precise de ser mantida por lei;
- Planos de continuidade: estes terão sido desenvolvidos para superar qualquer desastre e manter a continuidade do negócio.

❖ **Ativos de *software*: *s*oftware** de aplicação que implementa as regras de negócio da organização. A criação de software de aplicação é uma tarefa demorada. A integridade do software de aplicação é muito importante. Qualquer falha no software aplicativo pode ter impacto no negócio de forma adversa. E *software* de sistema [49];

❖ **Ativos físicos ou de *hardware*:** equipamento usado no dia-a-dia dos profissionais no centro hospitalar. Computadores, PDAs, portáteis e dispositivos médios, entre outros;

❖ **Ativos humanos:** qualquer pessoa que trabalhe diretamente ou indiretamente com a organização.

Depois dos ativos terem sido identificados, foi atribuído um responsável a cada um. A necessidade da identificação de um proprietário para cada ativo, é que este terá a responsabilidade por esse ativo e de responder por cada um deles. Ele será o responsável por proteger esses ativos de acordo com o valor atribuído e o risco potencial.

Qualquer adição ou modificação ao ativo de informação será realizado só com o consentimento do responsável pelo ativo. Só um proprietário do ativo será capaz de decidir sobre o valor do ativo dentro da organização. A menos que se saiba o valor de negócio correto do ativo, ninguém pode identificar o requisito de segurança do ativo [49].

Para cada um dos ativos que foram identificados com a ajuda de cada administrador, foram levantadas as seguintes informações: nome do ativo, a localização e o proprietário. Na sequência desta etapa, levantamento dos ativos, foram criadas posteriormente numa mesma tabela em *excel*, uma coluna para cada um dos três principais princípios de segurança da informação, CID e a cada um dos princípios foi atribuído um valor de acordo com o ativo em questão.

O valor atribuído teve primeiramente em conta o conjunto de entrevistas feitas anteriormente, onde estas possuíam bastante material, de forma a que o valor do ativo fosse primeiramente atribuído sem se recorrer aos administradores. Cada administrador no final deu a sua opinião sobre os valores atribuídos a cada ativo, pois melhor que

ninguém eles sabem qual o valor real de cada ativo. De forma a finalizar este trabalho de levantamento, realizou-se com os administradores conversas de forma a que eles validassem a informação referente às aplicações que fazem parte do seu núcleo de trabalho.

3.1.2 Identificação das Vulnerabilidades e Ameaças

Depois de se ter a fase do levantamento dos ativos concluída, foi a altura de identificar as vulnerabilidades e ameaças que fazem parte do ambiente que rodeia cada ativo. Esta identificação é realizada de forma a perceber qual é a probabilidade e o impacto que existiria se o par vulnerabilidade/ameaça fosse explorado.

As tabelas de vulnerabilidades e ameaças que se encontram na seção 8 e 7, respetivamente, do Apêndice 2 e as quais foram analisadas para se identificar os pares para cada ativo, foram construídas através da análise dos documentos [50], [51], [52], [53] e [54].

3.1.3 Determinação da Probabilidade e Impacto

A atribuição de valores à probabilidade e impacto teve em conta as tabelas da seção 12 e 13, do Apêndice 2, sobre a determinação da probabilidade e a determinação do impacto, respetivamente. Estas tabelas foram criadas com a ajuda do diretor do serviço dos sistemas de informação do centro hospitalar.

A probabilidade da existência do risco é influenciada pela fraqueza ou ausência de controlos. O risco é uma medida que combina a probabilidade de uma ameaça se materializar num ataque que explora uma vulnerabilidade, com o perigo que advém se isso realmente acontecer.

Apreciações do risco são usadas para descobrir quais as combinações de ameaça e vulnerabilidade tem um risco maior do que aquele que a organização quer aceitar. Tendo em consideração o valor do ativo e o custo do controlo a implementar, as organizações podem assim decidir como os deve tratar.

Cada apreciação do risco é muito característica porque as ameaças e vulnerabilidades que cada organização enfrenta estão inseridas num ambiente único que só aquela organização tem.

3.1.4 Determinação do Nível de Risco

Com a atribuição de valores à probabilidade e ao impacto de um par vulnerabilidade/ameaça que está associada a um determinado ativo e com o valor do ativo anteriormente atribuído, é possível obter o nível de risco correspondente ao ativo analisado.

A fórmula de cálculo do risco pode ser revista no Apêndice 2, onde esta é dada como sendo:

Nível de risco = Probabilidade x Impacto x Valor do ativo

Ao ser identificado o nível do risco, de acordo com a Tabela 27, do Apêndice 2, foi atribuído uma categoria de risco, que vai desde baixo a alto.

3.1.5 Recomendação de Controlos

Nesta parte do trabalho, analisou-se os riscos que foram encontrados e para cada um deles foi lhes associado um determinado controlo de forma a minimizar cada um dos riscos. Esta recomendação é importante para a organização pois assim poderá perceber as direções que devem seguir para mitigar os riscos mais críticos para a organização, das aplicações em estudo.

3.2 Geração de Métricas num Contexto Hospitalar

Com este caso de estudo ao centro hospitalar pretende-se mostrar o papel das métricas de risco de segurança da informação que podem ser geradas para suportarem as decisões que advêm de uma apreciação do risco. Este trabalho pretende mostrar a importância de haver um conjunto de métricas que sustentam a gestão do risco que as organizações procuram implementar e assim criar um modelo capaz de ser implementado na organização.

O trabalho dos gestores de segurança do centro hospitalar baseia-se na proteção de uma quantidade massiva de registos médicos e outras informações de pacientes e por conseguinte, quando eles se confrontam com um conjunto de riscos que devem ser mitigados, eles sabem que isso vai acarretar investimentos adicionais. Quando se fala em segurança da informação pode-se pensar que esta é somente uma questão do departamento de TI, mas este é um erro cometido muitas vezes. As organizações estão a enfrentar um número crescente de ameaças internas e externas e há uma escassez enorme de recursos e orçamento para os endereçar a todos. Assim, os administradores são cada vez mais solicitados para priorizar e justificar os seus pedidos para investimento [55].

Essa informação é apresentada posteriormente aos executivos e estes vão ter necessidade de saber o porquê desta ser importante e é aqui que começa o papel das métricas.

De acordo com [13], se as organizações não fossem muitas vezes assustadas através das notícias em comprarem soluções de segurança e estivessem concentradas fundamentalmente no que são questões de risco, as decisões relacionadas com a segurança da informação seriam somente baseadas em evidências de custo e uso de métricas para a gestão do risco de segurança da informação, tinham o seu papel específico. Todo este trabalho nasce desta questão, pois cada controlo selecionado para ser implementado deverá ter definido como ele será eficaz e quais as medições que avaliarão a sua eficácia, tudo deverá estar documentado no ponto que antecede a implementação. É assim que nasce as seguintes questões, quais os controlos que devem ser monitorizados, e como é que esses podem ser usados para fornecerem garantia às partes interessadas a quem está endereçada a informação, que será recolhida, analisada e tratada.

Este caso experimental foca-se principalmente na utilização de um método de medição que vai buscar os objetos de medição e atributos que surgem de resultados de apreciação e análise do risco, assim aos questionários e entrevistas realizadas no centro hospitalar.

As atividades necessárias para desenvolver medidas e medições devem ser estabelecidas e documentadas, incluindo o seguinte [23]:

- Definição do contexto da definição;
- Identificação de uma necessidade de informação;
- Seleção de um objeto de medição e seus atributos;
- Desenvolvimento de modelos de medição;
- Aplicação dos modelos de medição;
- Estabelecimento da recolha de dados e análise de processos e ferramentas;
- Estabelecimento da abordagem da implementação da medição e documentação.

Ainda segundo [23], a organização deve estabelecer objetivos de medição baseados num número de considerações, onde está incluído:

a) O papel da segurança da informação em suportar integralmente as atividades de negócio da organização e os riscos que estas enfrentam;
b) Requisitos legais, regulamentares e contratuais aplicáveis;
c) Estrutura da organização;
d) Custos e benefícios da implementação de medidas de segurança da informação;

e) Critérios de aceitação do risco pela organização;
f) A necessidade de comparar vários ISMS dentro da mesma organização.

Em [56] podemos encontrar alguns tipos de métricas: tempo tomado para realizar um *patch*, violações da política da organização, *endpoints* não infetados (percentagem de *endpoints* livres de *malware* e vírus), fugas de informação, redução do custo de segurança, formações do corpo profissional da organização, redução do tempo de inatividade não planeada do sistema, redução do número de vulnerabilidades conhecidas, o tempo médio para detetar incidentes de segurança, o tempo médio para resolver incidentes de segurança, número de utilizadores finais que estão a receber formação apropriada ao ambiente da organização e a redução do número de violações de acesso e autenticação.

O estudo descrito em [56] descobriu que somente 8 % dos gestores de segurança usam o desempenho do utilizador em testes, para verificar a retenção da consciencialização em segurança da informação como um meio de medir a eficácia da segurança.

O corpo profissional responsável pelos sistemas de informação está ainda focado primariamente em aspetos operacionais. E enquanto que muitos executivos estão focados em resultados mais visíveis, como a redução em fugas de informação, muito poucas organizações procuram gerar métricas mais preventivas. Gastos em relação ao orçamento total é utilizado como uma métrica fundamental para a eficiência de segurança por 49% dos inquiridos. Trinta e seis porcento dos gestores de segurança usam o retorno sobre investimentos em tecnologia de segurança como uma forma de medirem a eficiência da segurança [56].

Há metodologias diferentes que podem ser seguidas, quando se vai desenvolver métricas de segurança, mas não importa o modelo que vai ser seguido, deve ser garantido o propósito das métricas. Um forte suporte por parte da administração é necessário, porque pode parecer que a forma de desenvolver maneiras de contar coisas não é excessivamente complexo, a implementação atual e o uso de uma métrica e do seu sistema de medição pode ser bastante sobrecarregado. As métricas têm de ser desenvolvidas, adotadas, integradas e usadas em esforços de tomada de decisão [10].

De acordo com [20], o valor para a organização em usar as métricas é de longe aumentado se a geração das métricas nascer da medição daqueles aspetos do programa de SGSI que são considerados os mais importantes aquando de uma análise da necessidade de informação. A partir disto pode ser concluído que mesmo que uma norma tenha sido

desenvolvida para ser aplicada a cada organização, é preciso um conhecimento forte das metas de segurança da informação das organizações, assim como um entendimento da maturidade dos processos de segurança conectados a essas metas.

Uma vez que o controlo a ser avaliado tenha sido selecionado, as métricas serão geradas usando os dados disponíveis de forma a fornecerem um resultado que possa suportar o preenchimento completo, ou pelo menos uma parte, do controlo. Contudo, há um aspeto vital que tem de ser considerado quando a geração de métricas é baseada na informação disponível. As métricas têm de estar conectadas com as necessidades atuais dos profissionais de segurança que fazem parte da organização [20].

É necessário investir tempo a produzir o modelo de métricas e o seu programa, mas se este tempo for bem investido as métricas e o seu modelo podem ajudar a comunicar e a conduzir a uma melhoria do desempenho, medir a eficácia dos controlos de TI, diagnosticar problemas, suportar a tomada de decisões, guiar na alocação de recursos, demonstrar o estado de conformidade com regulamentos e leis e facilitar a comparação entre organizações do mesmo setor, principalmente quando esse setor tem metas que precisa de atingir [18].

O documento do NIST SP 800-55 [35], defende que "a maturidade do programa de segurança da informação da organização irá determinar o tipo de medidas que podem ser realizadas com sucesso. A maturidade do programa é definida pela existência e instituição de processos e procedimentos. À medida que um programa de segurança amadurece, as suas políticas tornam-se mais detalhadas e melhor documentadas, os processos que utilizam tornam-se, mais normativos e repetitivos e o programa irá produzir uma maior quantidade de informação que poderá ser usada para medição do desempenho.

Mas tem que se ter cuidado pois toda a informação no mundo não irá ajudar, se esta estiver numa forma que a audiência não a possa entender ou não dê as recomendações claras numa maneira persuasiva. A informação precisa de estar em slides com poucas palavras e muitas imagens, se esta for para ser apresentada à administração.

3.2.1 Desenvolvimento do Modelo de Métricas

Para o desenvolvimento do modelo de métricas, que consiste num conjunto de métricas de risco de segurança da informação, foram seguidas as orientações da norma ISO/IEC 27004, como já afirmado acima. Esta norma apresenta como partes integrantes do seu modelo de construção de métricas os seguintes constituintes: objeto de medição, atributos

do objeto de medição, métricas base, métricas derivadas, indicadores e resultados da medição, como pode ser visto na Figura 1 deste trabalho. Ligando todos estes constituintes existem: os métodos de medição, a função de medição, o modelo analítico e os critérios de decisão.

Sendo as métricas para a gestão de risco em segurança de informação o tema deste de trabalho, os objetos de medição que são usados no modelo apresentado pela ISO/IEC 27004, vêm da Tabela 1, referente à apreciação do risco realizada às cinco aplicações em estudo.

Extraindo um dos riscos encontrados, pretende-se aqui explicar o processo seguido para o desenvolvimento das métricas do Apêndice 3. Considerando o risco 'Divulgação de informação por falta de encriptação' o objeto de medição são as aplicações que têm informação confidencial dos pacientes e, portanto, o atributo do objeto de medição são as implementações de encriptação dentro das aplicações.

Tendo estes dois campos definidos é necessário verificar quais são as métricas básicas e quais são os métodos de medição que devem ser usados para obter a informação necessária para a geração das métricas. Dessa forma são consideradas duas métricas básicas com os seus respetivos modelos de medição:

- Número de aplicações contendo informação confidencial de pacientes, sendo possível obter esta informação através da contagem do número de aplicações contendo essa informação;
- Número de aplicações que contendo informação confidencial de pacientes tem encriptação de dados, sendo possível obter esta informação contando o número de aplicações que contendo informação confidencial de pacientes tem encriptação de dados.

Neste caso são consideradas duas métricas básicas, mas podem existir um número maior de métricas base, assim como pode não existir a necessidade de criar uma métrica derivada a partir das métricas básicas. Para este risco, que está a ser tomado como exemplo, para demonstrar a implementação da norma, é necessário gerar uma métrica derivada que vá fazer uso das duas métricas bases e que permite ter informação sobre o risco da perda de confidencialidade e integridade devido à falta de encriptação. A métrica derivada gerada é "Percentagem (%) de aplicações que contendo informação confidencial de pacientes tem os seus dados encriptados." e que possuí a seguinte função de medição

"(Número de aplicações que contendo informação confidencial de pacientes, têm encriptação) / (Número de aplicações que contêm informação de pacientes) *100". Possuindo estes campos preenchidos, os restantes que incluem 1) a definição do indicador, 2) o modelo analítico do próprio indicador, 3) o critério de decisão, 4) a interpretação do indicador e 5) o formato de apresentação são definidos, consoante o ambiente e sistema de cada organização. Os campos acima identificados vêm da proposta do modelo de construção de métricas apresentado pela ISO/IEC 27004, consultar Anexo 1.

O gestor responsável pelo desenvolvimento das métricas deverá ser capaz de estudar a organização e perceber o que melhor se adapta a ela, em cada um destes campos. Os campos 1), 2) e 5) depende da audiência a quem a métricas serão apresentadas e dessa maneira o gestor deve ser capaz de estudar a organização para saber qual a maneira mais apelativa para apresentar a informação às partes interessadas. Os campos 3) e 4) dependem maioritariamente das políticas ou orientações de cada organização, pelo que o gestor deve ter um bom conhecimento da organização para poder definir estes campos.

4 Resultados

Neste capítulo pretende-se apresentar os resultados quer da apreciação do risco, como o das métricas que foram escolhidas para dar suporte as decisões que saíram da apreciação do risco e que com elas se pretendeu gerar o modelo de métricas.

4.1 Apreciação do Risco

A primeira fase da dissertação passou por se fazer uma apreciação do risco de forma a se perceber quais os riscos que a organização enfrenta na área da segurança da informação. Esta não foi uma apreciação do risco tecnológica, mas organizacional de forma a perceber toda a estrutura do centro hospitalar e o ambiente de trabalho que envolve todo o corpo profissional.

A maior parte das organizações que fazem parte do setor da saúde, buscam essencialmente falhas técnicas. Contratam uma empresa externa e pedem que seja feita um *penetration testing*. Esta é uma ação que é de todo uma mais valia, porque há sempre coisas a melhorar. Mas aqui a mentalidade que é preciso mudar é que as organizações em muitos casos consideram que resolvendo os riscos que a ação de *penetration testing* revelou, já fizeram o seu trabalho e então está tudo bem.

Uma apreciação do risco à organização e todo o ambiente em que ela está envolvida mostra a imagem completa dos ativos no meio envolvente: ativos de informação, ativos de hardware, ativos de software e ainda os ativos humanos.

A Tabela 2 apresenta os principais resultados da apreciação do risco realizada a cinco aplicações que fazem parte do núcleo funcional do centro hospitalar. Por razões que se pode entender, não é divulgado o nome das aplicações em estudo nem os riscos que foram identificados para cada uma.

Dessa forma a Tabela 1 apresenta o resumo da apreciação do risco, tendo as seguintes colunas:

- **ID do controlo**: identificador utilizado pela organização para identificar cada um dos controlos que será recomendado de acordo com determinado risco.
- **ID do risco**: identificador utilizado pela organização para identificar cada um dos riscos encontrados. Reuniu-se vários ID de risco, de acordo com a identificação desse mesmo risco, não faz sentido termos ID separados se o risco que lhes está associado é o mesmo.

- **Nome do risco**: esta coluna apresenta o nome do risco encontrado. É através da identificação do risco que será possível recomendar um controlo.
- **Recomendação do controlo**: nesta coluna está disposto a recomendação dos controlos para mitigar os riscos identificados. A recomendação de um determinado controlo pode estar associada a um risco ou a mais riscos.
- ***Center for Internet Security – CIS*:** com esta coluna pretende-se justificar a recomendação do controlo tendo em consideração a missão que este centro e os trabalhos que desenvolve para a área da segurança da informação. Fazendo parte da missão do centro a identificação, desenvolvimento, validação, promoção e sustentação das melhores práticas em ciber segurança, é bom considerar os trabalhos desenvolvidos pelo centro e que servirão neste caso para justificar a recomendação dos controlos identificados.
- **Regulamento Geral de Proteção de Dados – RGPD**: nesta coluna pretende-se mostrar que a recomendação não é só uma medida de segurança que deveria ser cumprida, mas está disposto também num regulamento que foi tornado lei, as organizações terão de cumprir caso queram estar em conformidade com o mesmo.
- **ISO/IEC 27001**: aqui pretende-se mostrar que implementando a recomendação do controlo associada está-se a entrar em conformidade com os seguintes controlos abordados na ISO/IEC 27001. Isto é particularmente útil se a organização, neste caso o centro hospitalar, quiser um dia tentar uma certificação nesta norma.

Na Tabela 2, serão apresentadas análises adicionais que foram efetuadas, tendo como objetivo alertar as organizações da área da saúde para a necessidade de se trabalhar para uma maior segurança da informação no setor. Para a realização dessas análises foi estudado o novo RGPD [5], para se perceber o que se espera neste momento deste setor em termos de segurança. Foi também estudado o relatório do CIS [57], sobre os controlos que deveriam estar implementados para haver uma segurança efetiva nas organizações. Assim como o relatório [40], apresentado também pelo CIS, que propõe um conjunto de métricas, de onde os administradores podem escolher as que forem mais convenientes para a organização, ajudando assim a implementar este tipo de programas de medição da segurança da informação.

ID Controlo	ID Risco	Nome do Risco	Recomendação	CIS	GDPR	ISO 27001
C_1	RAI_1; RTapes_2	Divulgação de informação por falta de encriptação	Uso de controlos criptográficos	*CSC 13 - Data Protection*	**Artigo 32º, nº1, alínea a)** A pseudonomização e a cifragem dos dados pessoais; **Ver Recital (83) abaixo**	A.10.1.1 - A.10.1.2 A.18.1.3- A.18.1.4
	RApl_4	Divulgação de informação devido à não proteção do tráfego		*CSC 7 – Email and Web browser protections*		A.13.2.1 A.13.2.3
	RApl_5	Divulgação de passwords por causa da transmissão de passwords em texto claro				A.9.2.4 A.9.4.3 A.13.2.1 A.13.2.3
	RBD_6	Divulgação de passwords que pode acontecer devido à não proteção das tabelas das *passwords*		*CSC 13 - Data Protection*		A.10.1.1 - A.10.1.2
	RAI_3	Modificação não autorizada ou intencional	Uso de controlos criptográficos para garantir a integridade da informação			
C_2	RAI_2; RBD_1; RLogs_1	Comprometimento de informação confidencial por causa de falta de mecanismos de identificação e autenticação	Estabelecimento de processos fortes de identificação e autenticação	*CSC 5 - Controlled use of administrative privileges*	**Artigo 32º, nº 1, alínea b)** A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. **Recital (39)** Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.	A.9.1.1 A.9.4.2
	RAI_6; RPT_2	Divulgação e comprometimento de informação confidencial devido a uma gestão pobre de *passwords*				A.9.4.3
C_3	RAI_3	Modificação não autorizada ou intencional sem que haja registo dessas atividades	Estabelecimento de processos de registo de atividades	*CSC 6 - Maintenance, monitoring and analysis of audit logs*	**Artigo 5º, nº 1, alínea f)** Os dados pessoais são tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas ("integridade e confidencialidade"). **Recital (67)** Nos ficheiros automatizados, as restrições ao tratamento deverão, em princípio, ser impostas por meios técnicos de modo a que os dados pessoais não sejam sujeitos a outras operações de tratamento e não possam ser alterados.	A.12.4.1 – A.12.4.4 A.12.7.1 A.16.1.7
	RAI_4	Destruição de registos sem que haja registo dessa ação				
	RAI_5	Divulgação da informação explorando o facto que não há registos de acesso à informação			**Artigo 15º, nº 1, alínea c)** Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais.	

					Recital (87) Há que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular.	A.12.4.1 - 12.4.4 A.12.7.1 A.16.1.7
	RBD_5; RLogs_2	Acesso não autorizado à informação da base de dados por causa da falta ou pobre implementação de sistemas de registo de atividades internas				
C_4	RAI_7	Divulgação de informação através de cópias não controladas de informação	Uso de processos de controlos de cópias	*CSC 13 – Data Protection*	**Artigo 32º, nº 1, alínea b)** A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. **Recital (39)** Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.	
	RAI_8	Uso não autorizado de informação armazenada possibilitado pelo não controlo de cópias de segurança				
	RAI_9	Venda de informação pessoal que pode advir do não controlo de *downloads* de PDFs				
	RAI_10	Divulgação da informação que pode advir do não controlo de *downloads* de PDFs				
C_5	RBD_2	Divulgação e comprometimento de informação confidencial devido à não mudança das *passwords* por defeito da base de dados	Estabelecimento de uma política que preveja a alteração das passwords por defeito	*CSC 5 - Controlled use of administrative privileges*		A.9.2.4
C_6	RBD_3; RApl_1; RApl_2; RApl_3; ROS_1; RPT_3; RFW_1	Exploração automática de vulnerabilidades conhecidas devido à falta de instalação de *patches*	Gestão de *patches*	*CSC 18 - Application software security*		A.12.2.1 A.12.6.1
C_7	RInv_1	Probabilidade de acesso de dispositivos não autorizados devido à falta de atualização e revisão dos inventários	Gestão ativa de hardware na rede	*CSC 1 - Inventory of authorized and unauthorized devices*		A.8.1.1

C_8	RInv_2	Probabilidade de acesso de dispositivos não autorizados devido à falta de atualização e revisão dos inventários	Gestão ativa de software na rede	*CSC 2 – Inventory of authorized and unauthorized software*		
C_9	RTapes_1	Divulgação de informação causada pela eliminação ou reutilização de equipamentos sem processos de eliminação de informação corretos	Estabelecimento de um processo de eliminação e reutilização de equipamentos	*CSC 10 - Data recovery capability*	**Artigo 32º, nº 1, alínea b)** A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. **Recital (39)** Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.	A.11.2.1 A.11.2.7 - A.11.2.8
C_10	RTapes_3; RAut_1; RDC_1; RCO_1; RCO_2; RServ_1; RAS_1; RAA_1; RED_1; RGR_1; RGS_1; RExt_1; RHCP_1	Roubo devido ao uso inadequado ou descuidado dos controlos de acesso físicos ao *data center*	Uso de controlos de acesso físico, como é o caso da autenticação multi-fator.	*CSC 16 - Account monitoring and control*	**Artigo 32º, nº 1, alínea b)** A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. **Recital (39)** Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.	A.8.2.3 A.9.1.1 A.9.3.1 A.9.4.1 - A.9.4.3 A.12.3.1
C_11	RTapes_5	Uso não autorizado ou inadequado dos recursos de ativos ou ativos devido à falta de mecanismos de monitorização	Estabelecimento de processos de monitorização ou a existência de um período de retenção dos dados destes processos	*CSC 13 - Data Protection*		A.11.2.8 A.12.3.1
	RPL_1					A.11.2.8
C_12	RCO_3	Divulgação de informação devido à falta de mesas limpas	Estabelecimento de uma política sobre mesas limpas	*CSC 17 - Security skills assessment and appropriate training to fill gaps*	**Artigo 32º, nº 1, alínea b)** A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. **Recital (39)** Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.	A.7.2.2 A.11.2.9

C_13	RAS_3	Abuso de direitos por falta de separação de deveres	Monitorização da segregação de deveres	*CSC 13 - Data Protection*	**Artigo 32º, nº 1, alínea b)** A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. **Recital (39)** Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.	A.6.1.2
C_14	RHCP_2	*Phishing attacks* devido à falta de consciência de segurança	Formações de consciencialização sobre a segurança da informação: formações na área da segurança para os profissionais de saúde	*CSC 17 - Security skills assessment and appropriate training to fill gaps*	**Artigo 15º, nº 1, alínea c)** Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais. **Recital (87)** Há que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular.	A.7.2.2
C_15	RHCP_2	Divulgação de informação devido á falta de ecrãs limpos, devido à falta de consciencialização de segurança da informação	Estabelecimento de uma política sobre ecrãs limpos	*CSC 17 - Security skills assessment and appropriate training to fill gaps*	**Artigo 32º, nº 1, alínea b)** A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento. **Recital (39)** Os dados pessoais deverão ser tratados de uma forma que garanta a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas.	A.11.2.9

Tabela 1. Resumo dos riscos encontrados e recomendação de implementação de controlos

4.2 Levantamento de Métricas

No seguimento do trabalho, deu-se início à segunda parte da dissertação, esta consistiu num levantamento de métricas, que se enquadrava no ambiente do centro hospitalar e que teve como base a apreciação do risco. É deste levantamento que as métricas para o modelo a desenvolver foram escolhidas. O que era pretendido era conseguir agrupar um conjunto de métricas que ajudariam o centro hospitalar a escolher aquelas que mais se adequavam à organização, e dessa forma sensibilizar a administração para o investimento que não está a ser feito e poderá ser necessário fazer.

Nas seções abaixo, irá estar destacada cada recomendação de controlo, o porquê de ela ter sido considerada e quais as métricas que serviriam para avaliar esse mesmo controlo.

O sistema de informação do centro hospitalar não é maduro, podendo até afirmar-se que ele está a dar os seus primeiros passos, pelo que as métricas à primeira vista irão parecer bastante básicas. Mas como foi salientado anteriormente, deve-se começar devagar e evoluir o programa de métricas, contribuindo para o crescimento a partir deste ponto do SGSI. Esta é a primeira vez que o centro hospitalar está a pensar medir a sua segurança em termos da informação.

Há ainda uma outra questão que é preciso ter em conta, não se pretende dentro de cada um dos controlos abordados, explicar exaustivamente do que se trata ou o que deveria ser feito. O que se pretende fazer é abordar de uma forma genérica o controlo e explicar como é que as métricas escolhidas podiam ser medidas neste tipo de organização. Para uma visão mais completa do controlo deve consultar o trabalho publicado pelo CIS [57] sobre os controlos de segurança críticos para uma ciberdefesa eficaz. Na Tabela 1, existe uma coluna sobre este documento e que guia diretamente para o capítulo que deve ser analisado, dentro do mesmo.

Controlo 1 – Uso de controlos criptográficos

Tecnologia de informação na saúde permite que um utilizador malicioso obtenha e transfira informação de pacientes muito mais rápido do que com registos em papel. Outros erros que podem levar a desperdício, abuso e roubo de informação incluem falha a encriptar postos de trabalho ou portáteis, e discos com informação, com uma divulgação resultante das informações pessoais de saúde (*Personal Health Information - PHI*) [58].

Sendo a informação deste setor tão sensível é necessário que as organizações tenham consciência que o controlo de encriptação é um controlo de segurança de informação básico.

Riscos a mitigar
❖ Divulgação de informação devido à falta de encriptação: ❖ Divulgação de informação devido à não proteção de tráfego; ❖ Divulgação de passwords, resultante da transmissão de passwords em texto claro; ❖ Divulgação de passwords devido à não proteção das tabelas das passwords; ❖ Modificação não autorizada ou intencional.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de aplicações que têm os dados dos pacientes encriptados. ❖ Percentagem (%) de canais de comunicação controlados pela organização, que foram protegidos via encriptação. ❖ Percentagem (%) de passwords, PINs, e outras informações de autenticação que estão encriptadas.

Tabela 2. Levantamento de métricas para o uso de controlos criptográficos

As métricas que foram agrupadas para este controlo correspondem a métricas sobre a ausência ou não do controlo de encriptação. Como se depreende o centro hospitalar não aborda na sua política o dever das aplicações terem algum tipo de encriptação, pelo que se começou pelas métricas mais básicas: necessidade de saber se as aplicações que têm informação de pacientes estão protegidas por algum tipo de encriptação e se a informação em trânsito e informação de autenticação dos colaboradores estão protegidas. Não existindo outros controlos em lugar, que protejam a informação, o centro hospitalar está com um risco muito elevado, que deve ser mitigado, caso exista informação confidencial que não tem o nível mais simples de segurança.

A medição da ausência ou não do controlo de encriptação da informação, parece não trazer nada de muito concreto ao centro hospitalar, além de saber se tem ou não encriptação. Contudo, sem esta informação não podemos avançar para métricas mais maduras, como por exemplo, medir a robustez do algoritmo de encriptação.

Controlo 2 – Estabelecimento de processos fortes de identificação e autenticação

Os controlos de acesso precisam de ser definidos quer para indivíduos, quer para o grupo que englobam um conjunto de profissionais.

De acordo com [59], quando um novo membro chega à organização ele deve ser inscrito imediatamente e ser-lhe fornecido os direitos de acesso que ele irá precisar. Da mesma forma, quando um colaborador deixa a organização, as suas credenciais devem ser confiscadas e os seus direitos de acesso removidos nesse mesmo dia. Inspeções regulares ao sistema devem ser conduzidas para certificar que os níveis de acesso estão corretos e a aplicação está a trabalhar dentro das especificações que dela fazem parte.

Riscos a mitigar:
❖ Comprometimento de informação confidencial, resultante da falta de mecanismos de identificação e autenticação; ❖ Divulgação e comprometimento de informação confidencial, causados pela gestão pobre de *passwords*.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de colaboradores com acesso a contas partilhadas. ❖ Percentagem (%) de serviços de rede, que requerem requisitos de autenticação por parte dos colaboradores. ❖ Percentagem (%) de colaboradores que possuem o mesmo ID. ❖ Percentagem (%) de ID diferentes de acordo com a diferença entre as funções privilegiadas e atividades de negócio regulares. ❖ Percentagem (%) de colaboradores que têm a password guardada num ficheiro no computador. ❖ Percentagem (%) de colaboradores que têm a sua password em papel como forma de não esquecimento. ❖ Percentagem (%) de colaboradores que trocam passwords com os seus colegas. ❖ Percentagem (%) de aplicações que pedem autenticação com pelo menos dois fatores. ❖ Número de vezes que os ativos de informação e TI foram acedidos com sucesso sem que fosse completada uma função válida de identificação e autenticação.

Tabela 3. Levantamento de métricas para o controlo de estabelecimento de processos fortes de identificação e autenticação

Na análise realizada ao centro hospitalar, constou-se que este tem um sistema de gestão de identidades que trata da inserção, realocação dentro do centro hospitalar e remoção de

colaboradores de modo eficaz. Mas esta não é suficiente para eliminar todos os riscos que pode advir de processos de identificação e autenticação, e nesse sentido reuniu-se o conjunto de métricas apresentados na Tabela 3.

Controlo 3 – Estabelecimento de processos de registo e análise de atividades

Alguns acidentes diretamente relacionados com as características de software dos RES, tais como permitirem que múltiplos colaboradores adicionem texto na mesma nota de progresso, mas não permitindo cada fornecedor assinar, torna impossível a verificação do fornecedor do serviço atual ou a quantidade de trabalho realizada por cada colaborador [58].

Para proteger a integridade dos RES, é essencial assegurar a capacidade do sistema para identificar cada entrada, a data e a hora a que foram feitas, tais como alterações ou correções, o autor da mudança, e a razão para essa mudança ser feita. Alguns sistemas atribuem automaticamente uma data à entrada que foi feita. Outros permitem que utilizadores autorizados possam alterar a data de entrada de informação para a data da visita ou do serviço. Alguns sistemas permitem que os fornecedores façam alterações não datadas sem fazer distinção que a entrada original foi alterada. Se não há data nem hora na entrada original ou subsequentes alterações, a documentação que é fornecida para suportar os sistemas pode estar em causa. Em adição, se fornecedores não podem determinar a ordem dos eventos, a qualidade do cuidado ao paciente pode ser afetada ou comprometida [58].

Riscos a mitigar
❖ Modificação não autorizada ou intencional sem que haja registo dessas atividades; ❖ Destruição de registos sem que haja registo dessas atividades; ❖ Divulgação de informação explorando o facto de não existir registo de acessos à informação; ❖ Acesso não autorizado à informação da base de dados, causada pela falta ou pobre implementação de sistemas de registo de atividades.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Frequência média em que os registos de atividades foram revistos e analisados de forma a identificar atividades inapropriadas. ❖ Percentagem (%) de serviços de rede monitorizados. ❖ Percentagem de (%) de ID de colaboradores redundantes. ❖ Percentagem (%) de programas utilitários que têm processos de registo de atividades (*logging*). ❖ Percentagem (%) de áreas onde há registo de atividades (*logging*). ❖ Percentagem (%) de registo de atividades por número de aplicações. ❖ Percentagem (%) de registos de atividades das aplicações que são revistos num determinado período de tempo. ❖ Percentagem (%) de redes com processos de registo de atividades.

Tabela 4. Levantamento de métricas para o controlo de estabelecimento de processos de registo e análise de atividades

O conjunto de métricas levantadas basicamente na existência ou não de registos de atividades, que deveriam fazer parte de todas as aplicações com informação de saúde confidencial.

Controlo 4 – Uso de processos de controlo de cópias ou controlo do fluxo de informação

Os profissionais de saúde afirmaram que copiar e colar notas podem ser ações apropriadas, eliminando a necessidade de criar cada parte de uma nota ou voltar a entrevistar os pacientes sobre os seus registos médicos. Contudo, identifica-se ‘uso ilegítimo de copiar e colar na elaboração de relatórios’ como um problema [58].

Riscos a mitigar
❖ Divulgação de informação através de cópias não controladas de informação; ❖ Uso não autorizado de informação armazenada possibilitado pelo não controlo de cópias de segurança; ❖ Venda de informação pessoal que pode advir do não controlo de downloads de PDF; ❖ Divulgação de informação que pode advir do não controlo de downloads de PDF.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de postos de trabalho que impossibilitam o uso de *pens* ou discos por parte dos utilizadores. ❖ Percentagem (%) de postos de trabalho que impossibilitam o download de documentos/PDF.

Tabela 5. Levantamento de métricas para o controlo sobre o uso de processos de controlo de cópias

Como o centro hospitalar não tem nenhum processo de controlo de fluxo de informação, o conjunto das duas métricas pretende alertar para os controlos mais básicos, que podem ser implementados de forma a garantir que o centro hospitalar comece a tomar medidas de forma a controlar o fluxo de informação que sai fora do seu ambiente. É importante para o centro hospitalar perceber a extensão destes controlos e puder a partir daí começar a construir diretrizes quanto à permissão do uso de *pens* ou discos e ao *download* de ficheiros.

Controlo 5 – Estabelecimento de uma política que controla a alteração das *passwords* por defeito

A maior parte das instalações de aplicações, muitas vezes usam contas já criadas à priori pelos desenvolvedores dessas aplicações, e dessa forma algumas vezes as passwords dessas contas não são mudadas. Essa não alteração das *passwords* poderá permitir acesso a essas aplicações através dessas contas.

Riscos a mitigar
❖ Divulgação e comprometimento de informação confidencial, devido à não alteração de *passwords* por defeito.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de mudanças de configuração aprovadas e implementadas identificadas na última configuração automática de *software*.

Tabela 6. Levantamento de métricas para o controlo sobre o estabelecimento de uma política que preveja a alteração das passwords por defeito

Só será possível ter dados para a geração desta métrica se o centro hospitalar começar a documentar os processos de configuração de *software*. Assim que os dados estejam disponíveis, esta métrica permite perceber o risco que o centro hospitalar corre ao ter contas que ainda usam as suas *passwords* por defeito.

Controlo 6 – Gestão de *patches*

A latência de *patches* é o tempo entre um lançamento de um *patch* e implementação com sucesso desse mesmo *patch*. De acordo com [15], este é um indicador da disciplina de *patching* da organização e a sua habilidade de reagir a *exploits*, especialmente em organizações amplamente distribuídas com várias unidades de negócio, como é o caso do centro hospitalar.

Tal como acontece com as métricas básicas, a latência de *patches* pode mostrar dispositivos com a ausência de muitos *patches* ou então com *patches* desatualizados. Isto pode apontar para a necessidade de uma gestão de *patches* centralizado ou melhora de processos [60].

Riscos a mitigar
❖ Exploração de vulnerabilidades conhecidas devido à falta de instalação de *patches*.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de processos de controlo de *patching* num determinado período de tempo definido. ❖ Percentagem (%) de *patches* instalados onde se avaliaram os riscos da sua instalação. ❖ Percentagem (%) de *patches* instalados em postos de trabalho. ❖ Percentagem (%) de *patches* instalados em *Web Servers*.

Tabela 7. Levantamento de métricas para o controlo sobre a gestão de patches

Apesar das ameaças crescentes, como referido em [61], a maioria dos diretores de segurança e consequentemente a sua equipa, nem sequer pensam sobre as possíveis respostas a incidente, até que eles tenham experienciado uma intrusão de algum tipo. A maioria das organizações sentem-se relativamente seguras e então acreditam que os cibercriminosos não os irão atacar. Mas eles estão enganados, pois a maioria dos incidentes não estão mais focados numa organização em particular. A maior parte dos ataques são agora automatizados e estes disseminam-se com a intenção de causar danos a qualquer organização que esteja desprotegida contra esses ataques.

Controlo 7 – Gestão ativa de *hardware* na rede

A existência de inventários, neste caso recursos de *hardware*, é crucial para não perder noção dos dispositivos existentes no centro hospitalar e puder criar regras de acordo com os dispositivos conhecidos pela rede, impedindo que dispositivos desconhecidos possam se ligar ou fazer qualquer tipo de ação.

Riscos a mitigar
❖ A probabilidade de acesso a dispositivos não autorizados devido à falta de atualização e revisão dos inventários.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de dispositivos de *hardware* não cadastrados.

Tabela 8. Levantamento de métricas sobre o controlo de gestão ativa de hardware na rede

A métrica identificada pode ser medida através de *scan* feito à rede do centro hospitalar para que se verifique o número de dispositivos desconhecidos que estão ligados à rede.

Controlo 8 – Gestão ativa de *software* na rede

A gestão ativa de *software* segue a mesma linha de pensamento da gestão ativa de *hardware*, pois permite a implementação de controlos tendo em conta o *software* já conhecido pelo centro hospitalar e impedir dessa forma a ligação de *software* desconhecidos à rede.

Riscos a mitigar
❖ À grande probabilidade de uso de *software* não autorizado devido á falta de atualização e revisão dos inventários.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de *software* que está instalado na rede sem que esteja cadastrado nos inventários.

Tabela 9. Levantamento de métricas sobre o controlo de gestão de software na rede

Controlo 9 – Estabelecimento de um processo de eliminação e reutilização de equipamentos

A destruição e reutilização de equipamentos devem ser atividades escaladas, controladas e documentadas para que durante esse processo não se verifique a divulgação de informação confidencial.

Riscos a mitigar
❖ Divulgação de informação causada pela eliminação ou reutilização de equipamentos sem o estabelecimento de processos de eliminação de informação corretos.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de equipamento que antes de ser eliminado ou reutilizado, a sua informação e *software* foi eliminado de forma segura. ❖ Percentagem (%) de equipamento danificado que foi sujeito a uma avaliação de risco, para saber se podia ser destruído.

Tabela 10. Levantamento de métricas para o controlo sobre o estabelecimento de um processo de eliminação e reutilização de equipamentos

As duas métricas levantadas nascem da necessidade de haver a limpeza dos dispositivos quer eles sejam eliminados ou simplesmente reutilizados pela organização. Este processo deve ser realizado logo que seja decidido o destino do dispositivo, porque a prolongada estadia de um dispositivo para eliminação ou reutilização, pode levar ao esquecimento da realização do processo de eliminação da informação contida por eles.

Controlo 10 – Uso de controlo de acesso físico, como é o caso da autenticação multi-fator

Infelizmente, as organizações ainda se apegam à ideia que um campus aberto, ou a facilidade de acesso é uma abordagem positiva para as práticas de negócio e satisfação do corpo profissional. Adicionalmente, eles acreditam que a despesa para implementar um sistema de controlo de acesso é muito cara [59].

Controlar o acesso para fora e para dentro de um edifício ou campus não só impede um possível ataque terrorista, mas reduz a oportunidade para a prática de um crime ou a ocorrência de um ato violento. Além disso, promove uma sensação de segurança, não só para os empregados, mas também para outras pessoas que utilizam o espaço organizacional.

Um ambiente de trabalho que controla o acesso e identifica as pessoas exteriores à organização, proporciona paz aos empregados, e consequentemente promove a saúde espiritual da organização.

Como é que um programa de controlo de acessos e identificação das pessoas assiste o bem-estar de um indivíduo e a saúde espiritual de uma organização? Este promove uma cultura de proteção e segurança, reduzindo os riscos associados ao roubo de propriedade ou identificação de um indivíduo. Ele reduz o potencial de violência no local de trabalho, disputas domésticas e abuso por parte dos visitantes e da violência entre os funcionários.

Um programa de controle de acesso eficaz avalia os visitantes que utilizam as instalações e armazenam um registo de foto e documentos de identificação em caso de uma emergência ou do seu envolvimento em atividades criminosas. Ele ajuda a direcionar os visitantes que podem vaguear, restringindo o seu acesso apenas a áreas públicas e pode pré-autorizar compromissos como visitante através de um sistema informatizado de gestão de visitantes.

Além disso, um programa de acesso e identificação eficaz pode auditar o acesso de funcionários, visitantes e fornecedores, determinando quantas vezes é que eles entram em

áreas consideradas de alto risco. Ele pode fornecer a modificação de comportamento ou melhoria de comportamento através da promoção e educação dos empregados para o controlo de acesso apropriado e da cultura de identificação dentro da organização.

De acordo com [62], há uma tendência de os pacientes se sentirem agitados. Como pode o setor de saúde reduzir o número de incidentes violentos? Um dos métodos mais fáceis e eficazes é o controle do acesso e do uso de identificação.

A solução para a saúde é para controlar o acesso em áreas específicas dentro da instituição. Em certo sentido, classificando-os com base nos serviços de que necessitam e, em seguida, restringindo o seu acesso apenas às áreas que eles precisam para navegar, a fim de obter esses serviços médicos.

Muitas indústrias, como as indústrias de entretenimento e centros de saúde, requerem acesso aberto e ainda a manutenção de um programa de identificação. Sendo os agentes de segurança, responsáveis por verificar ID ou faces fotográficas, estes elementos podem não ajudar a identificar pessoas potencialmente problemáticas, embora se diga que os agentes de entrada impedem a entrada, no centro hospitalar, de pessoas problemáticas.

Riscos a mitigar
❖ Roubo de qualquer bem da organização, devido a um uso inadequado ou descuidado dos controlos de acesso físicos.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de incidentes de segurança física, permitindo a entrada não autorizada nas instalações contendo sistemas de informação. ❖ Percentagem (%) de perímetros de segurança protegidos com controlos de entrada apropriados, existem para proteger as áreas que processam a informação que suportam as informações clínicas. ❖ Percentagem (%) de equipamentos de TI expostos ao público sem controlos de segurança apropriados. ❖ Percentagem (%) de áreas onde é processada e armazenada a informação confidencial, que têm autenticação de pelo menos dois fatores.

Tabela 11. Levantamento de métricas para o controlo sobre o uso de controlos de acesso físico

Controlo 11 – Estabelecimento de processos de monitorização e existência de um período de retenção dos dados destes processos

A necessidade da existência destes processos de monitorização e retenção permitem controlar os dispositivos móveis que estão espalhados pelo centro hospitalar e que estão em constante contato com os pacientes. Num meio tão diversificado como é o centro hospitalar, é necessário assegurar algum nível de segurança visual, em caso de roubo do dispositivo, onde muitas vezes não se sabe se estes contêm informação lá dentro, resultando no risco da divulgação de informação.

Riscos a mitigar
❖ Uso não autorizado ou inadequado dos recursos de ativos ou ativos devido à falta de mecanismos de monitorização.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de locais não monitorizados onde estão localizados materiais/arquivos (media) contendo informação não encriptada. ❖ Percentagem (%) de áreas desocupadas que são monitorizadas o tempo todo.

Tabela 12. Levantamento de métricas para o controlo sobre o estabelecimento de processos de monitorização e existência de um período de retenção dos dados

Controlo 12 – Estabelecimento de uma política sobre mesas limpas

Com o estabelecimento de uma política sobre mesas limpas levará a que os colaboradores tenham cuidado com a informação ou objetos que deixam em cima dos seus postos de trabalho. Deve-se salientar que os locais de trabalho da maioria dos colaboradores do centro hospitalar, está em contato direto com o público permitindo se não houver cuidado com mesas limpas, a divulgação de informação a pessoas cuja intenção não está ao alcance do conhecimento dos colaboradores.

Riscos a mitigar
❖ Divulgação de informação devido à falta de mesas limpas.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de colaboradores que mantêm a informação sensível e crítica do negócio guardada num local seguro.

Tabela 13. Levantamento de métricas para o controlo sobre o estabelecimento de uma política sobre mesas limpas.

Controlo 13 – Monitorização da segregação de deveres

A segregação de deveres é um conceito chave de controlos internos que fazem parte de uma organização [63]. É imperativo que as organizações desenhem o sistema ou criem políticas de forma que nenhuma pessoa agindo sozinha, possa comprometer os controlos de segurança.

A segregação de deveres restringe a quantidade de poder ou influência mantida por qualquer indivíduo. Ela também assegura que os colaboradores não tenham responsabilidades que contribua para o conflito e que não sejam responsáveis por apresentem relatórios deles próprios, ou dos seus superiores. [63]

Da mesma forma, a responsabilidade individual para desenhar e implementar segurança, não deverá ser a mesma pessoa, que fica responsável por testar a segurança, conduzir auditorias de segurança monitorizar ou reportar em segurança.

Riscos a mitigar
❖ Abuso de direitos devido à falta de segregação de deveres.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
1. Percentagem (%) de colaboradores que podem aceder, alterar ou destruir informação sem serem detetados. 2. Percentagem (%) de colaboradores responsáveis pelo desenho e implementação de controlos de segurança assim como reportar sobre a eficácia desses controlos.

Tabela 14. Levantamento de métricas para controlo sobre a monitorização da segregação de deveres

O risco aqui identificado e que pode ser mitigado através do controlo A.6.1.2 presente em [43], poderá uma vez implementado, ser medido através da primeira métrica que revelará se esse mesmo controlo está a ser eficiente.

Controlo 14 – Formações de consciencialização para os profissionais de saúde

O valor da consciencialização em segurança da informação é especialmente vulnerável a criticismo. Consequentemente, a habilidade da equipa de segurança em educar e em enriquecer os seus colaboradores, nas suas responsabilidades de gestão do risco é fundamental para ou em qualquer estratégia de proteção do negócio. A consciencialização dos proprietários dos processos de negócio é um elemento fundamental numa estratégia de mitigação de risco.

A formação dos colaboradores pode ser um mecanismo efetivo para a mitigação de riscos. Quando o corpo operacional recebe formação sobre as espectativas e requisitos que um sistema de acesso e uso dos RES deve obedecer, assim como as consequências de um uso impróprio, reduz o potencial de risco [58]. O treino fornece um corpo fixo de conhecimento, enquanto a consciencialização pretende mudar comportamentos.

Riscos a mitigar
❖ *Phishing attacks* devido à falta de consciencialização de segurança do corpo profissional.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de pessoal de segurança dos sistemas de informação que tenham recebido formações de consciencialização em segurança da informação.

Tabela 15. Levantamento de métricas para o controlo sobre formações de consciencialização para os profissionais de saúde

Muitas outras métricas podiam ter surgido neste contexto. Há simulações de ataque que se estivessem implementadas na organização ou esta estivesse a pensar realiza-las, podiam inerentemente fornecer métricas. Tais simulações, que incluem ataques de *phishing*, USB caídas no chão ou deixadas em algum lado e até mesmo simulações de *social engineering*.

A segurança está relacionada com a mitigação dos riscos segundo a relação custo-eficácia, não com a prevenção de todas as falhas. Quando se está a lidar com pessoas, irá sempre haver uma perda relacionada na segurança.

Controlo 15 – Estabelecimento de uma política sobre ecrãs limpos

Este controlo segue a mesma linha de pensamento do controlo sobre o estabelecimento de uma política sobre mesas limpas. A saída de um colaborador do seu local ou posto de trabalho deixando o ecrã disponível para navegar no sistema do centro hospitalar ou então só na área de trabalho do colaborador em questão, leva a falhas de segurança muito grandes. O paciente, do qual não sabemos nada, pode aproveitar essa situação a seu favor, tornando-se ele um atacante do sistema, por negligência de um colaborador.

Riscos a mitigar
❖ Divulgação de informação devido à falta de ecrãs limpos, que surge o descuido do corpo profissional.
Caso o controlo fosse implementado, que métricas poderiam ser usadas para monitoriza-lo:
❖ Percentagem (%) de colaboradores que terminam de forma segura as sessões ativas aquando do fim da sua seção. ❖ Percentagem (%) de colaboradores que fazem log-off das aplicações ou serviços de rede que já não são necessários. ❖ Percentagem (%) de colaboradores que protegem os seus equipamentos de forma segura. ❖ Percentagem (%) de colaboradores que protegem os equipamentos que estão a seu cargo com uma autenticação segura.

Tabela 16. Levantamento de métricas para o controlo sobre o estabelecimento de uma política sobre ecrãs limpos

As métricas levantadas pretendem medir qual é a posição dos colaboradores quanto à execução de ações que promovem a segurança dos equipamentos onde estão a trabalhar.

4.3 Escolha das Métricas para o Modelo

Esta terceira e última parte deste trabalho consistiu num conjunto de entrevistas com os vários administradores, onde foi apresentado o levantamento de métricas da segunda parte do trabalho, para perceber quais as métricas que podiam ser geradas.

Na escolha das métricas seguiu-se as orientações definidas em [9] e dessa forma tentou-se desenvolver boas métricas tendo estas que ser específicas, mensuráveis, atingíveis, repetitivas e dependentes do tempo. De acordo com este artigo, métricas verdadeiramente úteis indicam o ponto de situação dos objetivos de segurança, tais como confidencialidade da informação, se estes estão a ser atingidos e se elas levam a ações que melhoram o programa de segurança completo da organização.

Tentou-se dessa forma criar métricas focadas em coisas específicas que se queriam medir e dessa forma foi possível saber aquilo que a organização precisa de se focar neste momento. Não importa a dimensão de algumas medições básicas pois estas são tanto esperadas quanto necessárias, de outro modo, será impossível demonstrar que alguma melhora foi realizada ou é requerida para propósitos corretivos [13].

As métricas escolhidas para o modelo, que se encontram listadas na Tabela 17. Para cada uma delas foi gerada segundo o modelo proposto pelo ISO/IEC 27004, e estão construídas da Tabela 28 à Tabela 36, do Apêndice 3.

Métricas que mostram risco:
❖ Percentagem (%) de colaboradores que podem aceder, alterar ou destruir informação sem serem detetados; ❖ Número médio de credenciais distintas por utilizador; ❖ Percentagem (%) de contas não correlacionadas por aplicação; ❖ Percentagem (%) de aplicações com registo de atividades: entrada na aplicação e operações realizadas; ❖ Percentagem (%) de aplicações que impossibilitam cópias de segurança; ❖ Percentagem (%) de contas partilhadas; ❖ Percentagem (%) de aplicações com controlos de *session time-out*; ❖ Percentagem (%) de aplicações que contendo informação confidencial de pacientes têm os seus dados encriptados; ❖ Percentagem (%) de *passwords* a que foi necessário fazer *reset*.

Tabela 17. Métricas escolhidas para o modelo

A gestão da segurança incorpora atividades administrativas e organizacionais necessárias para apoiar e proteger a informação e os ativos da organização, incluindo o desenvolvimento e a execução de políticas de segurança e os seus mecanismos de suporte: processos, normas, linhas de base e orientações. Ela engloba o desenvolvimento da segurança na organização, a gestão do risco, a seleção e implementação apropriada de controlos, governação e medição do desempenho. O centro hospitalar tem neste trabalho exemplos de aplicações de ações que devem ser tomadas para a criação do programa de segurança. Em adição a isto tudo, algumas das medidas podem ser usadas como potenciais KPI e podem ajudar formando parte de SLA quer com partes terceiras internas ou externas.

De forma a assegurar que as métricas seriam possíveis de se concluir assim como fornecerem a organização com informação valiosa, as métricas base foram selecionadas usando um processo de geração com a participação dos colaboradores responsáveis pela administração das aplicações em estudo do centro hospitalar dando enfase à validação das medições. Assim, as medições foram selecionadas de forma a que os dados necessários fossem recolhidos das fontes de informação disponíveis, sem haver a necessidade de aplicação de mais recursos do que aqueles já implementados. A consequência desta escolha é que as métricas não vão fornecer uma cobertura completa dos controlos correspondentes. Em vez disso, eles irão cobrir as partes dos controlos que são atualmente possíveis medir pela organização.

As métricas que foram geradas, pretendem usar informação disponível no sistema da organização, não pretendendo exigir mudanças organizacionais de forma a obter esses dados. A geração de métricas que requerem mudanças organizacionais exigem a participação e o suporte por parte dos gestores de segurança e administração [20]. O princípio orientador utilizado para gerar as métricas foi que sua a geração e uso deveria ser possível de realizar com recursos limitados. Usar um método onde a disponibilidade da informação é colocada um nível a cima, o uso de informação disponível, é recomendado em ordem a testar e melhorar a maturidade do programa de segurança da informação. As métricas cujo desenho é baseado nos dados que estão disponíveis podem mais tarde ser substituídas ou melhoradas para mostrar o cumprimento completo do controlo, uma vez que a maturidade do programa de segurança da informação vai evoluindo.

De salientar, que as métricas geradas são mais orientadas à parte técnica porque foram aquelas onde se podia obter a informação mais rapidamente e o centro hospitalar é uma organização menos madura em termos de segurança da informação. Se o centro hospitalar tivesse um programa de segurança da informação mais maduro teria sido possível e importante gerar métricas mais orientadas para processos e programas.

Começou-se com métricas básicas, esperando assim crescer lentamente, gerir expectativas e ser realistas. Fez-se o melhor possível com a informação que está disponível e então melhorar a partir delas.

Fazendo a análise das métricas geradas depara-se com a situação de algumas delas somente medirem a presença ou ausência de controlos técnicos, sem avaliarem a adequação ou resiliência do controlo em análise dentro do contexto da arquitetura de segurança ou ambiente operacional, é fácil entender que estas podem ser limitadas [42]. Mas como salientado anteriormente, são estas métricas básicas que farão com que o programa consiga ser implementado numa organização sem um SGSI maduro, ela tira valor destas e a partir desse modelo evolui para modelos mais robustos.

Um programa de métricas deve idealmente ser gerado para avaliar as partes mais críticas do programa de segurança da informação da organização, pelo que essas partes críticas foram identificadas aquando da apreciação do risco. Embora as métricas sejam limitadas, quanto à informação medida e o conhecimento que se pode tirar delas, considera-se que se conseguiu gerar um conjunto de métricas que irá possibilitar a monitorização nesta

etapa inicial de um SGSI no centro hospitalar, mas depois a partir destas é possível gerar métricas mais maduras.

Um dos pontos fracos que se tem de salientar deste trabalho, é o facto deste ter-se desenvolvido numa organização que como muitas outras em Portugal, faltam-lhe partes de um programa de um SGSI identificados na ISO/IEC 27001 da seção 4 à seção 9. De facto, se essas partes de um SGSI faltarem, isso irá tornar a tarefa da monitorização da eficácia do sistema muito difícil de implementar. Daí o modelo de métricas para a gestão do risco em segurança da informação ser constituído por métricas muito básicas, devido à falta de maturidade do programa.

Alternativamente há metodologia seguida, os controlos iniciais poderiam ter sido selecionados diretamente da ISO/IEC 27001 por uma pessoa representativa da gestão de segurança da informação. Contudo, isto iria requerer, contudo, um esforço muito maior por parte dessa pessoa, e devido às limitações de tempo do corpo profissional, isso não foi uma opção viável.

Deve ser salientado que a abordagem não foi de todo baseada na criação de métricas para medir qualquer atividade que seja possível. Medições demandam recursos e por essa razão estas devem ser sempre motivadas pela necessidade de conhecimento sobre a segurança da informação na organização [46].

5 Conclusões

Uma ideia que se deve levar deste trabalho e que é defendida por vários autores, é que sem métricas adequadas, não se consegue provar verdadeiramente o valor de um programa de segurança. O uso de métricas permite que uma organização tenha um conhecimento verdadeiro da saúde do seu programa de segurança, porque cada atividade pode ser medida de uma maneira quantificável. As métricas são usadas em atividades de governação porque elas permitem que sejam feitas as melhores decisões estratégicas. No conjunto de métricas geradas o centro hospitalar será capaz de criar estratégias para uma maior segurança da informação e consequente conformidade com o RGPD, que ele tem de endereçar neste momento. O centro hospitalar terá assim, não só a visão do que precisa de fazer (quais os controlos mais importantes a implementar), mas terá um modelo para medir o quão bem estão a fazer essa implementação e assim melhorar continuamente.

Os resultados obtidos têm em consideração as contribuições e objetivos deste trabalho. Foi possível implementar a metodologia seguida pela ISO/IEC 27005 e é também apresentado o relatório da metodologia seguida, sendo dessa forma mostrado na prática como é que esta norma pode ser implementada. A apreciação realizada desenvolveu-se conforme o previsto possibilitando a obtenção das variáveis críticas que devem ser monitorizadas.

Depois de se ter obtido as variáveis críticas estas foram tomadas como os objetos na implementação da ISO/IEC 27004, para que dessa forma fosse possível obter as métricas de risco de segurança da informação e mostrar a implementação prática desta norma. Sendo uma das lacunas a falta de trabalhos práticos que mostrem a verdadeira essência da norma quando aplicada numa organização e sabendo que a ISO/IEC 27004 somente dá orientações sobre a implementação destes programas de medição da segurança da informação, este trabalho surge tentando colmatar a ausência destes trabalhos práticos. Mas neste trabalho existe a consciência de que este acaba por ter sido desenvolvido sobre um SGSI pouco maduro, acabando por demonstrar que um SGSI mais maduro permite desenvolver métricas que trazem conhecimento mais valioso para as organizações.

Pode-se concluir que este centro hospitalar representa várias organizações de saúde em Portugal e dessa forma verifica-se que este setor ainda precisa de muito trabalho no desenvolvimento de SGSI para protegerem de forma segura a informação dos pacientes. Através da apreciação do risco realizada é possível extrair que este é um setor ainda com

muitos riscos para mitigar e recursos a que devem recorrer de maneira a que possam realmente proteger a informação e entrar em conformidade com o RGPD. As dificuldades encontradas no desenvolvimento das métricas surgiram devido aos poucos recursos existentes para obter a informação precisa para as gerar ou então, só ser possível obter essa informação através de questionários que acabam por gastar muito tempo e envolver muitos colaboradores, e ainda considerando que as respostas podem não coincidir com a realidade. No entanto, as métricas de risco de segurança da informação mostraram-se úteis e viáveis dentro do sistema da organização. Úteis porque vão de encontro com a necessidade de informação sobre a quantificação dos riscos que necessitam de mitigar e viáveis porque são possíveis obter somente com os recursos disponíveis.

5.1 Trabalho Futuro

Era importante, como trabalho futuro a esta dissertação, rever as métricas que não foram possíveis ser geradas para ver se revertendo alguma delas poderão representar KPI de valor substancial para a organização e consequentemente a administração. De seguida, deve-se realizar uma análise para determinar a quantidade de investimento que deveria ser realizado para gerar essas métricas, tudo em vista a tornar a organização mais madura e possuir mais conhecimentos sobre as suas atividades e processos.

Seria importante seguir de perto o modelo e conseguir avaliar a metodologia proposta e qual a sua validade para as organizações do setor da saúde e se é possível a partir de métricas de risco de segurança da informação geradas, conseguir a maturação ou evolução do SGSI da organização. Por outro lado, seria também muito importante considerar a replicação do mesmo caso de estudo a outros centros hospitalares. Perceber se é possível aplicar a mesma metodologia, se os resultados são os mesmos, se as métricas geradas seriam mais maduras, o que indicaria um sistema de informação naturalmente mais maduro. Ter um quadro com vários estudos ao setor da área da saúde seria importante para criar uma metodologia própria para o setor estudado. Essa metodologia seria um apoio para a iniciação de processos de gestão de risco e medição da segurança da informação dentro das organizações.

6 Referências Bibliográficas

[1] ISO/IEC 27000, “Information technology — Security techniques — Information security management systems — Overview and vocabulary,” *October*. 2014.

[2] Instituto Português da Qualidade, “DNP ISO Guia 73 Gestão do risco - Vocabulário.” 2011.

[3] R. Barabanov, S. Kowalski, and L. Yngstrom, “Information security metrics: Research directions,” 2011.

[4] R. Cambra, “Metrics for Operational Security Control.” SANS Institute, 2004.

[5] W. K. Brotby, *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*. Taylor & Francis Group, LLC, 2009.

[6] Conselho da União Europeia, “Regulamento Geral sobre a Proteção de Dados,” 2016.

[7] B. Filkins, “Health Care Cyberthreat Report: Widespread Compromises Detected, Compliance Nightmare on Horizon,” 2014.

[8] G. Bell and M. Ebert, “Health Care and Cyber Security: Increasing Threats Require Increased Capabilities,” 2015.

[9] S. C. Payne, “A Guide to Security Metrics,” 2006.

[10] S. Harris, *CISSP All in one: Exam Guide*, 6 edition. McGrawHill, 2013.

[11] RSA, “Cybercrime and the Healthcare Industry.” EMC2, 2013.

[12] J. Breier, P. Hofbauer, and L. Hudec, “Risk Analysis supported by Information Security Metrics,” *International Conference on Computer Systems and Technologies*, 2011.

[13] S. Wright, “Measuring the Effectiveness of Security using ISO 27001,” 2006.

[14] G. Grandy, Rick; Serene, “NASA: A report of a field.”

[15] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, First Edit. Addison-Wesley, 2007.

[16] L. G. Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash, “Security Metrics Guide for Information Technology Systems,” 2003.

[17] R. B. Vaughn, R. Henning, and A. Siraj, “Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy,” *Proc. 36th Annu. Hawaii Int. Conf. Syst. Sci. HICSS 2003*, 2003.

[18] D. Rathbun, “Gathering Security Metrics and Reaping the Rewards.” SANS Institute,

2009.

[19] S. Haas, S. Wohlgemuth, I. Echizen, N. Sonehara, and G. Müller, "Aspects of privacy for electronic health records," *Int. J. Med. Inform.*, vol. 80, no. 2, pp. e26–e31, 2010.

[20] K. Lundholm, J. Hallberg, H. Granlund, K. Lundholm, and J. Hallberg, "Design and Use of Information Security Metrics: Application of the ISO/IEC 27004 Standard," 2011.

[21] "Introduction to ISO 27002," 2013. [Online]. Available: http://www.27000.org/iso-27002.htm. [Accessed: 15-Oct-2016].

[22] ISO/IEC 27002, "Information technology - Security techniques - Code of practice for information security controls." 2013.

[23] ISO/IEC 27004, "Information technology - Security Techniques - Information security management - Measurement," 2009.

[24] D. Kosutic, "O Ciclo PDCA foi removido das novas normas ISO?," *27001 Academy*, 2014. [Online]. Available: http://advisera.com/27001academy/pt-br/blog/2014/04/15/o-ciclo-pdca-foi-removido-das-novas-normas-iso/. [Accessed: 28-Sep-2016].

[25] S. Jafari, F. Mtenzi, R. Fitzpatrick, and B. O. Shea, "Security Metrics for e-Healthcare Information Systems : A Domain Specific Metrics Approach," *Int. J. Digit. Soc.*, vol. 1, no. 4, pp. 238–245, 2010.

[26] D. Melancon, "Make Your Security Metrics Matter To The Business | The State of Security," *The State of Security*. [Online]. Available: http://www.tripwire.com/state-of-security/security-data-protection/make-your-security-metrics-matter-to-the-business/. [Accessed: 07-Apr-2016].

[27] D. Melancon, "Don't Be Baffled by BS Security Metrics," *The State of Security, Tripwire*, 2013. [Online]. Available: https://www.tripwire.com/state-of-security/risk-based-security-for-executives/connecting-security-to-the-business/dont-be-baffled-by-bs-security-metrics/. [Accessed: 07-Apr-2016].

[28] Tripwire, "Are Security Metrics Too Complicated for Management?," *The State of Security, Tripwire*. [Online]. Available: http://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/are-security-metrics-too-complicated-for-management/. [Accessed: 07-Apr-2016].

[29] D. Melancon, "Security metrics : 5 tips," *The State of Security, Tripwire,* 2012. [Online]. Available: http://www.tripwire.com/state-of-security/security-data-protection/security-metrics-5-tips/. [Accessed: 07-Apr-2016].

[30] D. Melancon, "Countermeasures , Weather Forecasts , and Security Metrics," *The State of*

Security, *Tripwire*, 2012. [Online]. Available: http://www.tripwire.com/state-of-security/security-data-protection/countermeasures-weather-forecasts-and-security-metrics/. [Accessed: 07-Apr-2016].

[31] Tripware, "To Navigate Your Security Program, Measure Well," *The State of Security, Tripwire*, 2012. [Online]. Available: http://www.tripwire.com/state-of-security/security-data-protection/to-navigate-your-security-program-measure-well/. [Accessed: 07-Apr-2016].

[32] V. Haran, "HDFC Bank's ISO 27004 compliant security metrics a boost toward GRC," *Computer Weekly*, 2012. [Online]. Available: http://www.computerweekly.com/feature/HDFC-Banks-ISO-27004-compliant-security-metrics-a-boost-toward-GRC. [Accessed: 06-Apr-2016].

[33] NP ISO 31000, "Gestão de Risco - Princípios e linhas de orientação (ISO 31000:2009)." 2013.

[34] NIST SP 800-30 Revision 1, "Guide for Conducting Risk Assessments," 2012.

[35] NIST SP 800-55 Revision 1, "Performance Measurement Guide for Information Security," 2008.

[36] D. Shanthamurty, "NIST SP 800-30 Standard for Technical Risk Assessment: An Evaluation," 2011. [Online]. Available: http://www.computerweekly.com/tip/NIST-SP-800-30-standard-for-technical-risk-assessment-An-evaluation. [Accessed: 22-Sep-2016].

[37] W. Jansen, "Directions in Security Metrics Research, NISTIR 7564," 2009.

[38] G. Eckes, *The Six Sigma Revolution: How General Electric and Others Turned Process Into Profits*. John Wiley & Sons, 2001.

[39] M. Sajko, "Measuring and Evaluating the Effectiveness of Information Security," in *Risk Assessment and Management*, AcademyPublish.org, 2012, pp. 402–411.

[40] CIS, "A Measurement Companion to the CIS Critical Security Controls," 2015.

[41] M. H. S. Peláez, "Measuring effectiveness in Information Security Controls," 2010.

[42] D. S. Herrmann, *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI*. 2007.

[43] ISO/IEC 27001, "Information technology - Security techniques - Information security management systems - Requirements." 2013.

[44] C. Kreitner and M. Dickson, "Report of the Best Practices and Metrics Teams," 2005.

[45] CIS, "The CIS Security Metrics," 2010.

[46] R. Barabanov, S. Kowalski, and L. Yngstrom, “Information Security Metrics State of the Art,” 2011.

[47] N. Shukla and S. Kumar, “A Comparative Study on Information Security Risk Analysis Practices,” *Spec. Issue Int. J. Comput. Appl. Issues Challenges Networking, Intell. Comput. Technol.*, vol. 12, no. January, pp. 57–67, 2017.

[48] eHealth Ontario, “Guide to Information Security for the Health Care Sector.” 2010.

[49] I. E. Group, “Identifying and classifying assets,” *Network Magazine*, 2002. [Online]. Available: http://www.networkmagazineindia.com/200212/security2.shtml. [Accessed: 04-Mar-2016].

[50] ISO/IEC 27005, “Information technology — Security techniques — Information security risk management,” 2011.

[51] IGT, “ISMS Risk Assessment Manual Version 1.4,” 2002.

[52] D. Kosutic, “Catalogue of Threats and Vulnerabilities,” *Advisera Academy*. [Online]. Available: http://advisera.com/27001academy/knowledgebase/threats-vulnerabilities/. [Accessed: 29-Apr-2016].

[53] WatchGuard Technologies, “Top 10 Threats to SME Data Security,” 2008.

[54] BSI EN ISO 27799, “Health informatics — Information security management in health using ISO / IEC 27002 (ISO 27799:2008),” 2008.

[55] M. C. Mont, Y. Beresnevichiene, D. Pym, and S. Shiu, “Economics of Identity and Access Management: Providing decision support for investments,” *2010 IEEE/IFIP Netw. Oper. Manag. Symp. Work. NOMS 2010*, pp. 134–141, 2010.

[56] Tripwire, “Key Metrics for Risk - Based Security Management,” *The State of Security, TripwireTripwire*, 2013. [Online]. Available: http://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/key-metrics-for-risk-based-security-management/. [Accessed: 07-Apr-2016].

[57] CIS, “The CIS Critical Security Controls for Effective Cyber Defense,” 2015.

[58] Centers for Medicare & Medicaid Services, “Program Integrity Issues in Electronic Health Records: An Overview,” 2015.

[59] B. Scaglione, “Why Access Control and Identification is Healthy for Your Organization,” *Security*, 2011. [Online]. Available: http://www.securitymagazine.com/articles/82379-why-access-control-and-identification-is-healthy-for-your-organization. [Accessed: 07-Apr-2016].

[60] S. Berinato, "A Few Good Information Security Metrics," *CSO Online*, 2005. [Online]. Available: http://www.csoonline.com/article/2118152/metrics-budgets/a-few-good-information-security-metrics.html.

[61] S. Kaplan, "Incident Response: When Bad Things Happen to Good Companies," *CSO Online*, 2003. [Online]. Available: http://www.csoonline.com/article/2115899/network-security/incident-response--when-bad-things-happen-to -good-companies.html. [Accessed: 03-Jun-2016].

[62] B. Scaglione, "Preventing Healthcare Crime With Access Control and ID," *Security*. [Online]. Available: http://www.securitymagazine.com/articles/83342-preventing-healthcare-crime-with-access-control-and-id. [Accessed: 07-Apr-2016].

[63] K. Coleman, "The key to data security : Separation of duties," *Computer World*, 2008. [Online]. Available: http://www.computerworld.com/article/2532680/technology-law-regulation/the-key-to-data-security--separation-of-duties.html. [Accessed: 28-May-2016].

Apêndice 1 – Material Desenvolvido para as Entrevistas

Aqui se pode encontrar as perguntas que foram colocadas aos vários intervenientes entrevistados no centro hospitalar. Estas perguntas foram colocadas de forma a se puder compreender a organização, o seu sistema e o ambiente de cada uma das aplicações em estudo.

Pretendeu-se obter a perceção de cada um dos intervenientes responsáveis pelas aplicações em estudo e do respetivo diretor dos sistemas de informação do centro hospitalar. A entrevista inicial com cada de dos responsáveis, está representada na Tabela 18. Cada uma das perguntas expostas foram realizadas a cada um dos administradores. Deste primeiro conjunto de entrevista, pode-se ter noção do verdadeiro ambiente de um centro hospitalar.

Foi possível entender como cada um dos administradores entende um ambiente hospitalar, como vêm a segurança da aplicação pela qual são responsáveis e qual é a ideia deles de uma apreciação do risco e no que ela podia ajudar a melhorar o ambiente hospitalar.

As perguntas foram criadas tendo em conta que a limitação de acesso à informação num ambiente de saúde, encontra-se dividida por vários grupos: médicos, enfermeiros, auxiliares de saúde, voluntários, administradores e diretores.

A.9.1: ***Business requirements of access control:*** to limit access to information and information processing facilities.
1. Quem tem acesso ao quê dentro do centro hospitalar? 2. Quando os médicos (exemplo de um grupo de profissionais) acedem a informações de pacientes, estes têm acesso a informações dos seus pacientes ou tem informações de outros pacientes.
A.9.1.1: ***Access control policy:*** *an access control policy shall be established, documented and reviewed based on business and information security requirements.*
1. Qual é política de controlo de acesso que o centro hospitalar tem? 2. Quais as áreas que são consideradas mais críticas em termos de informação? 3. Se há uma política de controlo de acessos ela está documentada? Há um plano para a sua revisão? 4. A política de controlo de acessos é transmitida às várias partes interessadas?

5. Em que momento é que essa informação é transmitida?

A.9.1.2 Access to networks and networks services: *users shall only be provided with access to the network and network services that they have been specifically authorized to use.*

1. Quando médicos, enfermeiros, administração têm acesso a redes ou serviços de rede, eles têm restrições ou toda a rede está aberta?
2. Que informação está disponível na rede?
3. Há procedimentos de autorização para determinar quem pode aceder a determinadas redes e redes de serviços?
4. Há processos de controlo para proteger o acesso às conexões da rede?
5. Há monitorização do uso dos serviços da rede?
6. Que requisitos de autenticação é que são necessários?
7. Que meios é que existem para aceder às redes e aos serviços das mesmas?

A.9.2.2 ***User access provisioning:*** *a formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.*

1. Quando um médico, enfermeiro ou outro profissional de saúde muda de posto de trabalho, o que corresponde a uma mudança do conteúdo de informação a que tem acesso, esta mudança nos acessos à informação é realizada?
2. Se há qual é a plataforma/*software* utilizada?
3. Há periodicidade na revisão dos direitos de acesso com os proprietários dos sistemas de informação ou serviços?
4. Manutenção de um registo central com os direitos de acessos concedidos a cada utilizador?
5. Verificação se o nível de acesso concedido está de acordo com as políticas de controlo de acesso do centro hospitalar?
6. Quando é concedido direitos de acesso a um determinado utilizador, alguma autorização é obtida por parte dos proprietários dos sistemas de informação ou serviços?

A.9.2.3 ***Management of privileged access rights:*** *The allocation and use of privileged access rights shall be restricted and controlled.*

1. Este processo no centro hospitalar é controlado por quem?
2. Existem direitos privilegiados de acesso?

3. Quem pode ter acesso?
4. Há requisitos para a expiração de direitos privilegiados de acesso?
5. As competências dos utilizados com direitos privilegiados de acesso são revistas regularmente de forma a verificar se elas estão em linha com os seus deveres?
6. Existe algum processo de autorização de privilégios de controlo de acesso?
7. Existe algum registo central com os registos dos privilégios dos diretos de acesso concedidos?
8. Se existem privilégios de controlo de acesso, qual é base que é seguida para a concessão destes direitos especiais?
9. Privilégios de controlo de acesso devem ser definidos para um ID diferente daqueles usados para atividades de negócio regulares?

A.9.2.4 ***Management of secret authentication information of users:*** *the allocation of secret authentication information shall be controlled through a formal management process.*

1. Há um processo que faça a proteção da informação de autenticação que deve de ser secreta?
2. Quem controla e gere esse processo?
3. Quantas pessoas é que têm acesso?
4. Há algum documento que tem de ser assinado para manter a confidencialidade da informação de autenticação segura?
5. Como é que essa informação é transmitida?
6. Há alguma forma de saber que o utilizador recebeu a informação de autenticação?
7. A informação de autenticação aquando da instalação de sistemas ou software é alterada no final da instalação?
8. Aonde é que essa informação fica guardada?
9. Qual é o tipo de informação de autenticação usado? (*passwords*, chaves criptográficas, *smart cards*)

A.9.2.5 ***Review of user access rights:*** *asset owners shall review user's access rights at regular intervals.*

1. O processo de revisão dos direitos de acesso de cada colaborador é realizado?
2. Se sim, quantas vezes por ano?

3. Se não, como se sabe que os direitos de acesso de cada colaborador estão corretos e não têm mais direitos dos que aqueles que eram devidos?
4. As mudanças feitas ao nível de contas privilegiadas são registadas para revisão periódica?
5. Os direitos de acesso são revistos periodicamente em intervalos regulares e de qualquer mudança, tal como promoções, despromoções ou despedimento?
6. Os direitos de acesso são revistos ou realocados quando um utilizador muda de uma posição para a outra dentro do centro hospitalar?
7. As autorizações para privilégios de controlo de acesso são revistas em períodos de tempo frequentes?
8. Alocações privilegiadas são revistas em períodos regulares para assegurar que privilégios não autorizados foram obtidos?

A.9.2.6 ***Removal or adjustment of access rights:*** *the access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.*

1. Como é processada a mudança de direitos de acesso, que deve acontecer quando há uma saída de um profissional interno ou externo, promoção ou despromoção?
2. Como se processa a saída de utilizador de um grupo? Os seus direitos de acesso são removidos? Os utilizadores que integram o grupo são avisados para não partilhar mais informação com o utilizador que saiu?

A.9.3 ***User responsibilities:*** *the objective is to make users accountable for safeguarding their authentication information.*

1. Os colaboradores são responsáveis por guardar as suas credenciais de autenticação?

A.9.3.1 ***Use of secret authentication information:*** *Users shall be required to follow the organization´s practices in the use of secret authentication information.*

1. O centro hospitalar tem práticas que devem ser seguidas pelos colaborados, no que toca à informação de autenticação, como é o caso das *passwords*?
2. Há verificação de que as práticas estão a ser seguidas?
3. Há troca de *passwords*?
4. As *passwords* são escritas em papeis como forma de não esquecimento?

5. Há restrições a quando da escolha de uma *password*?
6. Há obrigações para se mudar a password frequentemente?
7. Qual é o processo usado para armazenar as *passwords*?
8. Há processos que verificam a qualidade das *passwords*?

A.9.4 *System and application access control:* *the objective is to prevent unauthorized access to systems and applications*

1. Há alguma forma de prevenção e monitorização dos acessos autorizados e não autorizados?

A.9.4.1 *Information access restriction:* *access to information and application system shall be restricted in accordance with the access control policy.*

1. Que políticas de controlo o centro hospitalar apresenta em termos de restrições de controlo de acesso?
2. Há algum processo que controle quem acedeu a determinada informação?
3. Há algum processo que controle a informação a que um determinado utilizador acedeu?
4. Há algum processo que limita a informação contida na saída, de acordo com os controlos de acesso desse utilizador?
5. Existem controlos de acesso físicos e lógicos que isolem aplicações sensíveis, dados de aplicações ou sistemas?

A.9.4.2 *Secure log-on procedures:* *where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.*

1. Que processos de *log-on* existem implementados?
2. Que políticas de controlo de acesso se debruçam sobre os processos de *log-on*?
3. Onde é que o *log-on* é mais crítico?
4. Existe algum método de autenticação alternativo às passwords?
5. O design das aplicações e dos sistemas está desenhado para minimizar as oportunidades de acesso não autorizado?
6. O processo de *log-on* fornece mensagens de ajuda que pode ajudar um utilizador não autorizado a obter acesso?
7. Há registo das tentativas de *log-on*, quer sejam de acesso ou não sucesso?
8. Como é feita a transmissão das passwords através da rede?
9. As sessões são terminadas depois de um período definido de inatividade?

10. Há restrição de quantas tentativas existem no processo de *log-on*?
11. A informação de *log-on* só é validada depois de toda a informação ser inserida?
12. Se ocorrer um erro durante o processo de *log-on*, o sistema ou aplicação indica qual é a parte da informação que está correta ou incorreta?

A.9.4.3 ***Password management system:*** *password management systems shall be interactive and shall ensure quality passwords.*

1. Há algum processo que controle a qualidade das passwords que são geradas?
2. Onde a qualidade das passwords é mais relevante em termos de política no hospital?
3. Há um registo de passwords anteriormente usadas que previne a reutilização das *passwords*?
4. O armazenamento dos ficheiros das passwords é feito separadamente da informação do sistema ou aplicação?
5. O armazenamento e a transmissão são feitos de forma segura?

A.9.4.4 ***Use of privileged utility programs:*** *the use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.*

1. O acesso a programas que monitorizam e controlam outros programas, têm restrições de acesso?
2. Como é que este processo é realizado?
3. São usados processos de identificação, autenticação e autorização para programas utilitários?
4. Há separação entre programas utilitários e software de aplicações?
5. Há limitação do uso dos programas utilitários a número reduzido de utilizadores autorizados?

A.9.4.5 ***Access control to program source code:*** *access to program source code shall be restricted.*

1. O acesso ao código fonte dos programas está restrito?
2. Há políticas nesse sentido?
3. As bibliotecas fontes dos programas são mantidas nos sistemas operativos?
4. Há registo dos acessos feitos às bibliotecas fontes dos programas?

A.10.1.1 ***Policy on the use of cryptographic controls:*** *a policy on the use of cryptographic controls for protection of information shall be developed and implemented.*
1. Existe alguma política sobre o uso de controlos criptográficos?
A.10.1.2 ***Key management:*** *a policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.*
1. Nos processos de encriptação existentes na organização existe alguma política ou procedimentos implementados quanto à proteção das chaves de encriptação?
A.11.1 ***Secure areas:*** *the objective is to prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.*
1. As instalações de processamento da informação têm limitações de acesso? (aqui entra o caso do controlo de acessos físicos, como é que o centro hospitalar restringe este acesso?) 2. Quem lá acede? *3.* E ao que tem acesso?
A.11.1.1 ***Physical security perimeter:*** *security perimeters shall be defined and used to protect areas that contain either sensitive data or critical information and information processing facilities.*
1. Há perímetros físicos de segurança? 2. Há formas de restrição de acesso a diferentes áreas de segurança? 3. Existem sistemas de deteção de intrusos? *4.* Existem alarmes?
A.11.1.2 ***Physical entry control:*** *secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.*
1. Como é controlada a entrada e saída de visitas? 2. A entrada em áreas de alta segurança é controlada por algum processo? 3. Há algum controlo de acesso nessas áreas? *4.* Existe algum livro, físico ou eletrónico, com *logs* de acesso?

A.11.1.3 ***Securing offices, rooms and facilities:*** *physical security for offices, room and facilities shall be designed and applied.*
1. Os edifícios onde se encontram atividades de processamento de informação estão sinalizados na parte de fora dos edifícios? *2.* O público pode aceder a essas áreas?
A.11.1.4 ***Protecting against external and environmental threats:*** *physical protection against natural disasters, malicious attack or accidents shall be designed and applied.*
1. Existem proteções contra ameaças externas e ambientais: incêndios, inundações, terramotos, explosões, etc.?
A.11.1.5 ***Working in secure areas:*** *procedures for working in secure areas shall be designed and applied.*
1. É permitido trabalhar em áreas seguras sem supervisão? *2.* As áreas seguras são fisicamente fechadas e periodicamente inspecionadas aquando de períodos de férias e outros períodos longos?
A.11.2.9 ***Clear desk and clear screen policy:*** *a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.*
1. Como é guardada a informação de negócio crítica e sensível? 2. Há alguma política nesse sentido? 3. Que processo é realizado antes da entrada num período de férias? 4. Onde é que a informação é guardada? 5. Como são deixados os computadores quando uma pessoa deixa o seu posto temporariamente, num período de férias ou de um dia de trabalho para o outro? 6. Há alguma política quanto ao uso de impressoras para digitalizar, fotocopiar, etc. documentos? 7. Há algum processo que remove informação classificada ou sensível das impressoras imediatamente depois de realizar a sua função? 8. As impressoras usam código para serem utilizadas?

Tabela 18. Primeiro conjunto de entrevistas.

Na Tabela 19 da seção do anexo podemos encontrar as perguntas que foram colocadas depois de uma primeira análise feita a organização. Estas perguntas já foram mais direcionadas para o ambiente específico da organização e para o ambiente das aplicações em estudo e tendo em consideração as várias leituras efetuadas no decorrer do trabalho:

1. Existem alguns requerimentos ou restrições na configuração de serviços de rede Wi-Fi aquando do uso de redes domésticas?
2. A informação de autenticação aquando da instalação de sistemas ou *software* é alterada no final da instalação?
3. A informação de autenticação dos utentes é enviada via e-mail, mas como se processa em relação à informação de autenticação das pessoas com direitos de acesso privilegiados?
4. A má configuração de *software* é uma situação recorrente? Isto pode levar a problemas a nível de controlo de acessos que podem ser explorados por hackers.
5. A SPMS dá diretrizes sobre o uso da PEM? Ela forneceu alguma política sobre como é que deveria proceder com as credenciais e os cartões?
6. Aquando do uso do computador para trabalhar remotamente, são tomadas algumas precauções para evitar acesso não autorizado a esses dispositivos? Uso de técnicas criptográficas ou reforço nos modos de autenticação?
7. As áreas mais críticas têm videovigilância ou algum processo de segurança mais apertado?
8. As áreas seguras são fisicamente fechadas e periodicamente inspecionadas aquando de períodos de férias e outros períodos longos?
9. As bibliotecas fontes dos programas são mantidas nos mesmos servidores que as aplicações?
10. As competências dos utilizadores com direitos de acesso privilegiados são revistas regularmente de forma a verificar se elas estão em linha com os seus deveres?
11. As impressoras usam códigos para serem utilizadas?
12. Como é guardada a informação de negócio crítica e sensível?
13. Como é justificada cada vista de informação por um médico, etc.? Há alguma prova de que há uma relação legítima para que se tenha acedido a essa informação?

14. Como é que são deixados os computadores quando uma pessoa deixa o seu posto temporariamente, num período de férias ou de um dia de trabalho para outro?
15. Como estão protegidas as tabelas de *logs*?
16. Como se processa a atribuição dos direitos de acessos privilegiados?
17. É permitido trabalhar em áreas seguras sem supervisão?
18. É possível aceder à rede do hospital através do telemóvel, ou qualquer outro dispositivo móvel?
19. É possível aceder a redes externas ao centro hospitalar através das estações de trabalho?
20. É possível enviar informação confidencial de utentes para qualquer pessoa?
21. Erros de manutenção são frequentes?
22. Existe algum documento assinado que mostre as responsabilidades de cada administrador em relação às aplicações em estudo?
23. Existe algum processo de autorização de privilégios de controlo de acessos?
24. Existe algum registo central com os registos dos privilégios dos direitos de acesso concedidos?
25. Existem casos em que várias pessoas são responsáveis pela mesma aplicação? À forma de saber quando cada um acedeu ou as credenciais de acesso são as mesmas?
26. Existem *logs* de ativação e desativação de sistemas de proteção como é o caso de antivírus e sistemas de deteção de intrusões?
27. Existem *logs* de mudanças na configuração dos sistemas?
28. Existem proteções contra ameaças externas e ambientais: incêndios, inundações, terramotos, etc.?
29. Existem sistemas de deteção de intrusos? Alarmes, etc.?
30. Há algum documento que tenha de ser assinado ou que tenha de ser lido informando a confidencialidade da informação de autenticação deve ser preservada? (no caso de acessos privilegiados?)
31. Há algum processo que remove informação classificada ou sensível das impressoras imediatamente depois de realizar a sua função?
32. Há alguma política quanto ao uso de impressoras para digitalizar, fotocopiar documentos?

33. Há alguma proteção contra DDoS?
34. Há alguma separação de redes, redes de serviços ou há uma só rede?
35. Há algumas políticas de controlo de acesso que se debrucem sobre os processos de *log-on*?
36. Há controlos implementados para que as pessoas não caiam em ataques de engenharia social?
37. Há *logs* pelo menos no acesso de utilizadores privilegiados?
38. Há necessidade de existirem revisões dos direitos de acesso?
39. Há perímetros físicos de segurança?
40. Há procedimentos de autorização para determinar quem pode aceder a determinadas redes e redes de serviços?
41. Há registo das tentativas de *log-on*, quer sejam de *log-on* bem-sucedidos ou não?
42. Há registos dos acessos feitos às bibliotecas fontes dos programas?
43. Há requisitos para a expiração dos direitos privilegiados de acesso?
44. Já existiram casos de roubo/desaparecimento de equipamento?
45. Já existiram casos de vandalismo a equipamento por parte de pessoas internas ou externas?
46. Nas estações de trabalho há impedimentos para instalação de software por parte dos colaboradores dessas estações de trabalho?
47. O acesso a programas que monitorizam e controlam outros programas, têm restrições de acesso? Como este processo é realizado?
48. O acesso ao código fonte dos programas está restrito? Há políticas nesse sentido?
49. O centro hospitalar tem colaboração com universidades? Como é feito o controlo de acessos destas às redes? Por exemplo, investigação.
50. O design das aplicações e dos sistemas está desenhado para minimizar as oportunidades de acesso não autorizado?
51. O hospital tem algum sistema de voluntários em colaboração com ele? Como se processa isto em termos de controlo físico e eletrónico? A aplicação Gestão de Identidades contempla estes casos?
52. O hospital tem algum sistema de voluntários em colaboração com ele?
53. Onde é que a informação é guardada?

54. Os enfermeiros também podem aceder à informação contida no PACS?
55. Possuem áreas onde uma pessoa só pode entrar se for acompanhada?
56. Privilégios de controlo de acesso devem ser definidos para um ID diferente daqueles usados para atividades de negócio regulares, este controlo está implementado?
57. Quais são os meios que existem para aceder às redes e aos serviços das mesmas?
58. Qual é a referência usada pelo hospital para a sincronização do relógio? *'The correct stting of computer clocks is important to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinar cases.'*
59. Quando na gestão de horários para um médico, enfermeiro, etc., sai do seu horário, a sessão desse utilizador é fechada ou um médico que vá para a mesma estação de trabalho pode continuar a trabalhar nessa sessão? Ou num pior caso um enfermeiro, um auxiliar ou um voluntário pode mexer nessa sessão?
60. Quando se acedem às tabelas de logs é possível modificá-las ou apagá-las?
61. Quantas pessoas é que têm acesso à informação de autenticação dos utilizadores? E dos administradores?
62. Que processo é realizado antes da entrada num período de férias?
63. Quem pode aceder aos *data centers* e ao que tem acesso?
64. Quem tem direitos de acessos privilegiados?
65. Sabem se existem trocas de passwords entre profissionais de saúde?
66. Se existem privilégios de controlo de acesso, qual é a base que é seguida para a concessão destes direitos especiais?

Tabela 19. Segundo conjunto de entrevistas.

Apêndice 2 – Metodologia da Apreciação do Risco

Metodologia da Apreciação do Risco

Data	Versão	Criado por	Descrição da atualização
21.07.2016	0.1	Manuela Faria	Criação desta metodologia.

1. Propósito

O propósito que leva à criação desta metodologia é estabelecer um mecanismo que deverá sempre ser seguido aquando da realização de uma apreciação do risco dentro do centro hospitalar em estudo. O estabelecimento de uma metodologia é extremamente importante pois permitirá que os resultados de análises do risco posteriores sejam comparáveis entre si.

Como esta foi a metodologia seguida na avaliação de 5 aplicações que fazem parte do sistema do centro hospitalar, é necessário salientar que esta deve ser revista, se numa apreciação do risco posterior forem incluídas mais aplicações ou o sistema completo para análise.

Os resultados de uma apreciação do risco fornecem um entendimento sobre o risco da segurança da informação que pode afetar operações organizacionais, ativos, indivíduos e outras organizações que trabalham com o centro hospitalar.

O propósito da identificação dos riscos é determinar o que pode acontecer se existir uma potencial perda, e assim ganhar uma visão global sobre como, onde e porque é que essa perda pode acontecer.

2. Definição do âmbito

O objetivo de conduzir apreciações do risco deve ser claramente documentado. O objetivo destas deve passar por cumprir com a política estabelecida pela organização, requisitos regulamentares ou legislativos. O âmbito deve ser a organização inteira, uma parte da organização ou só um sistema de informação específico.

A definição do âmbito precisa de ter em conta as dependências que uma apreciação do risco tem com as outras partes da organização, outras organizações, fornecedores ou qualquer outra entidade fora do programa de segurança da informação.

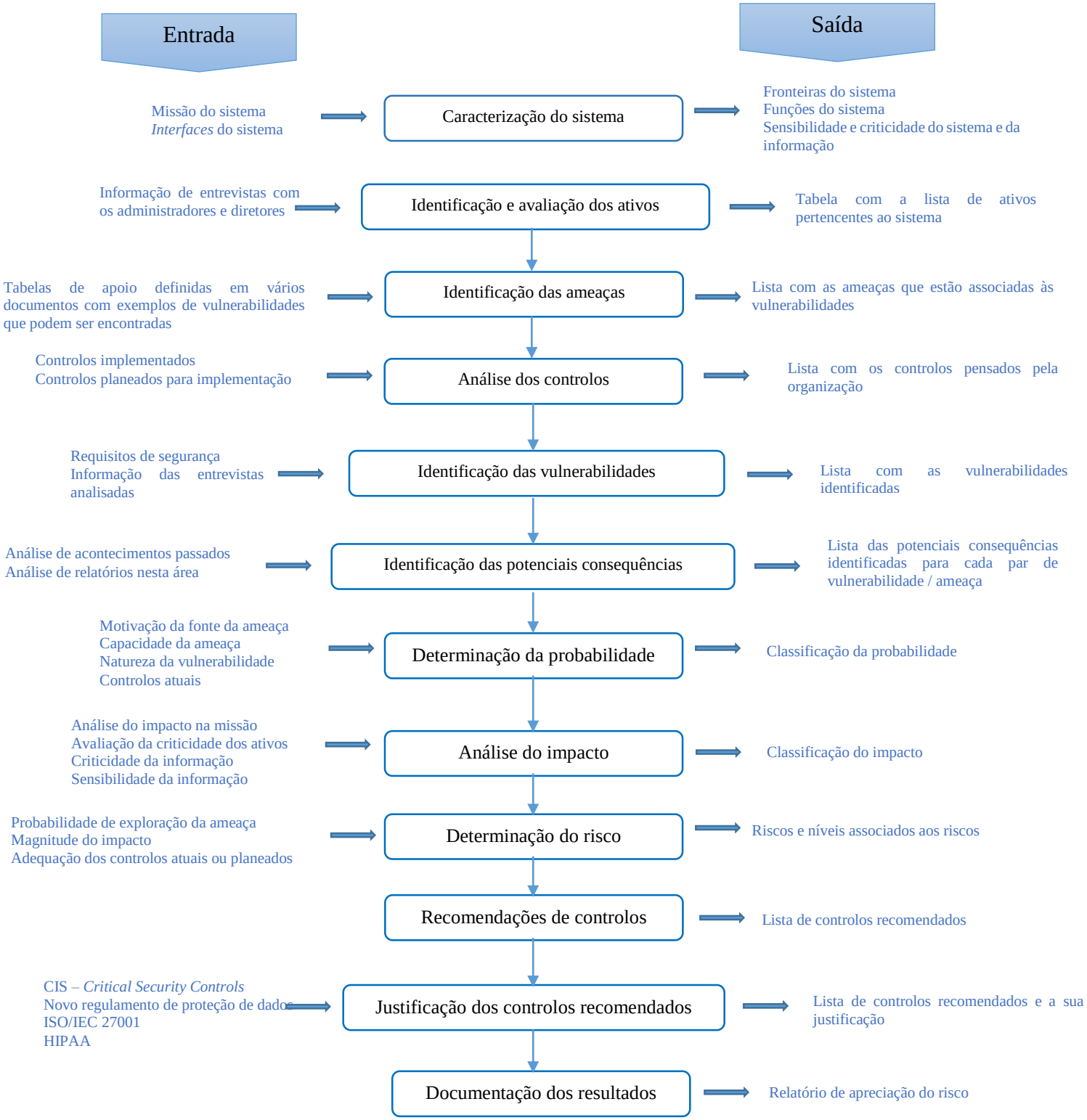
O âmbito da apreciação do risco deve ser identificado em termos de aplicabilidade organizacional, prazo suportado e considerações, quer de arquitetura, quer tecnológica.

3. Termos e definições

Ameaça	Causa potencial de um incidente indesejável, o qual pode causar perigo a um Sistema ou à organização.
Análise do risco	Processo destinado a compreender a natureza do risco e a determinar o nível do risco.
Apreciação do risco	Processo global de identificação do risco, de análise do risco e de avaliação do risco.
Ativo	Ativo é tudo aquilo que tem valor para uma organização.
Auditoria de gestão do risco	Processo sistemático, independente e documentado de obtenção de evidências e sua avaliação objetiva de forma a determinar o grau de adequação e eficácia de uma estrutura de gestão do risco, ou de uma parte selecionada desta.
Avaliação do risco	Processo de comparação dos resultados da análise do risco com os critérios do risco para determinar se o risco e/ou respetiva magnitude é aceitável ou tolerável.
Confidencialidade	Propriedade que garante que a informação não ficará disponível ou será divulgada a indivíduos, entidades ou processos não autorizados.
Consequência	Resultado de um evento que afeta objetivos.
Controlo	Medida que modifica o risco.
Critérios do risco	Termos de referência em relação aos quais a significância de um risco é avaliada.
Descrição do risco	Caracterização estruturada do risco contendo, usualmente, quatro elementos: as fontes, os eventos, as causas e as consequências.
Disponibilidade	Propriedade que representa estar acessível e possível de utilizar sob demanda de entidade autorizada.

Dono do risco	Pessoa ou entidade com responsabilização e com a autoridade para gerir o risco.
Estabelecimento do contexto	Definição dos parâmetros externos e internos a ter em consideração quando se gere o risco e se define o âmbito e o critério do risco para a política de gestão do risco.
Fonte do risco	O elemento que, por si só ou em combinação com outros, tem o potencial intrínseco de originar um risco.
Gestão do risco	Atividades coordenadas para dirigir e controlar uma organização no que diz respeito ao risco.
Identificação do risco	Processo de pesquisa, de reconhecimento e de descrição dos riscos.
Integridade	Propriedade de exatidão e totalidade.
Matriz do risco	Ferramenta que permite ordenar e visualizar os riscos por definição de intervalos de consequência e possibilidade.
Nível do risco	Magnitude de um risco ou combinação de riscos, expressa em termos de combinação de consequências e respetivas possibilidades.
Probabilidade	Medida da possibilidade de ocorrência expressa por um número entre 0 e 1, onde 0 representa a impossibilidade e 1 representa a certeza absoluta.
Requisitos de segurança	Requisitos de segurança descrevem objetivos de negócio no que diz respeito à proteção de ativos e informação.
Risco	Efeito da incerteza no alcance dos objetivos.
Segurança da informação	Preservação de confidencialidade, integridade e disponibilidade.
Vulnerabilidade	Propriedade intrínseca de algo que resulta na suscetibilidade a uma fonte de risco que pode conduzir a um evento com consequência.

4. Fluxograma da metodologia



5. Caracterização do sistema

Caracterizar um sistema de TI estabelece um âmbito para o esforço da apreciação do risco, delimita fronteiras para a autorização operacional, e fornece informação essencial (*hardware*, *software*, *interfaces* do sistema, divisões responsáveis e colaboradores de suporte, entre outros) para definir o risco.

Uma boa caracterização do sistema permite compreender quais são os resultados desejados pela organização e dessa forma é mais fácil perceber e selecionar um conjunto adequado de controlos de segurança da informação para o respetivo ambiente da organização.

6. Identificação e avaliação dos ativos

Depois da caracterização do sistema, onde se consegue ter uma visão geral do sistema e dos seus constituintes, está na altura de fazer o levantamento dos ativos. A identificação dos ativos deve passar por identificar tudo o que está ligado à aplicação, direta ou indiretamente. Assim, devem ser considerados como principais categorias de ativos: ativos de informação, ativos de *hardware*, ativos de *software* e ativos humanos.

É importante identificar todos os ativos que são relevantes para o negócio da organização e atribuir um valor relativo a cada um. Este processo torna mais fácil decidir quais os ativos que devem ser protegidos, daqueles que não precisam de tanta proteção. Se houverem muitos ativos para gerir, agrupar ativos semelhantes ou relacionados em categorias que possibilitam a gestão, pode tornar o processo de análise do risco mais simples.

Deve-se fazer o levantamento da seguinte informação relativa aos ativos:

- Categoria do ativo;
- Nome do ativo;
- Descrição do ativo;
- Proprietário;
- Localização.

A avaliação dos ativos tem por base os pilares em que assenta a segurança dos sistemas de informação, sendo estes a confidencialidade, integridade e disponibilidade. Passa também por atribuir um valor relativo de negócio a cada um dos ativos identificados. É importante notar que o valor de negócio não é só o valor monetário do ativo, mas também

inclui o potencial impacto no negócio devido à sua perda (por exemplo, perda informação protegida de saúde causa não conformidade com o Regulamento Geral de Proteção de Dados). Cada requisito legal e/ou contratual relacionado com cada ativo e com a organização deve também ser identificado.

A meta da avaliação dos ativos é atribuir os valores de impacto para os ativos no contexto da confidencialidade, integridade e disponibilidade. O valor do impacto deve ser baseado no pior cenário, usando uma escala apropriada para a organização e deve ser validado pelo responsável pelo ativo. A importância de fazer o levantamento dos responsáveis pelos ativos, é revelada através da ajuda que esta dá em assegurar a adequada segurança da informação, uma vez que os proprietários ao validarem ou atribuírem um valor ao ativo está implicitamente a mostrar o nível de segurança que este deve ter.

Abaixo encontram-se as tabelas usadas para avaliar cada categoria de ativos. Em vez de usar uma tabela genérica para fazer a avaliação, foram construídas três tabelas que avaliam em separado os ativos de informação, os ativos de *hardware* e *software* e os ativos humanos.

Critérios de avaliação dos ativos de informação			
	Confidencialidade	**Integridade**	**Disponibilidade**
Alta (3)	Informação que é muito sensível e privada, de alto valor para a organização e destinada a ser usada somente por indivíduos nomeados. A divulgação não autorizada de tal informação pode causar dano severo (exemplos, responsabilidade legal e financeira, impacto competitivo adverso, perda do nome de marca). Exemplos incluem, informação sobre os preços do cliente, informação relacionada com fusão ou aquisição, estratégia de marketing.	A degradação da integridade é inaceitável.	O ativo/informação é requirido numa base de 24 horas/7 dias da semana.
Média (2)	Informação pertencente à companhia e não disponível para divulgação pública ou a partes terceiras. A divulgação não autorizada da informação pode causar um prejuízo limitado à organização.	Há um impacto significante no negócio se o ativo, se a exatidão e integridade completa da informação for degradada.	Há um impacto significativo no negócio se o ativo/informação não está disponível por um período maior de 48 horas.
Baixa (1)	Informação não sensível disponível para divulgação pública. O impacto de divulgação não autorizada de tal informação não deve causar qualquer prejuízo à organização. Exemplos incluem comunicados de imprensa, cartas da empresa, informação publicada no website da empresa.	Há um impacto mínimo no negócio se a exatidão e integridade completa da informação for degradada.	Há um impacto mínimo no negócio se o ativo/informação não está disponível por um período maior de 7 dias.

Tabela 20. Critérios de avaliação usados nos ativos de informação

Critérios de avaliação dos ativos de *hardware* ou *software*			
	Confidencialidade	**Integridade**	**Disponibilidade**
Alta (3)	Informação processada / armazenada / transportada ou serviços prestados pelo ativo no processo de negócio tem requisitos de confidencialidade como alta.	Dependência e confiança dos serviços prestados por um ativo particular num processo de negócio é alta. Informação processada / armazenada / transportada ou serviços prestados por um ativo num processo de negócio tem os requerimentos de integridade como alta.	Impacto da indisponibilidade de um ativo num processo de negócio é alta. Informação processada / armazenada / transportada ou serviços prestados por um ativo num processo de negócio tem requisitos de disponibilidade como alta.
Média (2)	Informação processada / armazenada / transportada ou serviços prestados pelo ativo no processo de negócio tem requisitos de confidencialidade como média.	Dependência e confiança dos serviços prestados por um ativo particular num processo de negócio é média. Informação processada / armazenada / transportada ou serviços prestados por um ativo num processo de negócio tem os requerimentos de integridade como média.	Impacto da indisponibilidade de um ativo num processo de negócio é média. Informação processada / armazenada / transportada ou serviços prestados por um ativo num processo de negócio tem requisitos de disponibilidade como média.
Baixa (1)	A informação processada / armazenada / transportada ou serviços prestados pelo ativo no processo de negócio tem requisitos de confidencialidade como baixa.	Dependência e confiança dos serviços prestados por um ativo particular num processo de negócio é baixa. Informação processada / armazenada / transportada ou serviços prestados por um ativo num processo de negócio tem os requerimentos de integridade como baixa.	Impacto da indisponibilidade de um ativo num processo de negócio é baixa. Informação processada / armazenada / transportada ou serviços prestados por um ativo num processo de negócio tem requisitos de disponibilidade como baixa.

Tabela 21. Critérios de avaliação usados nos ativos de hardware ou software

Critérios de avaliação de ativos humanos			
	Confidencialidade	**Integridade**	**Disponibilidade**
Alta (3)	O papel do empregado ou parte terceira identificada tem acesso a todos os tipos de ativos de informação incluindo ativos de informação classificados como 'confidenciais' ou ativos de IT classificados como 'críticos'. Uma quebra de segurança por indivíduos para que o papel está atribuído irá afetar severamente as operações de negócio.	O papel ou parte terceira identificada tem privilégio para mudar ativos de informação classificados como 'confidenciais' ou mudar a configuração dos ativos de IT classificados como 'críticos'. Uma quebra de segurança por indivíduos a quem o papel está atribuído irá afetar severamente as operações de negócio.	Indisponibilidade do indivíduo a quem o papel está atribuído irá afetar severamente as operações do negócio.
Média (2)	O papel ou parte terceira identificadas têm acesso limitado aos ativos de informação classificados como 'internos' e 'públicos'. Uma quebra de segurança por indivíduos a quem o papel está atribuído irá afetar moderadamente as operações do negócio.	O papel ou parte terceira identificada tem privilégio para mudar ativos de informação classificados como 'internos' ou 'públicos'. Uma quebra de segurança por indivíduos a quem o papel está atribuído irá afetar moderadamente as operações de negócio.	Indisponibilidade do indivíduo a quem o papel está atribuído irá afetar moderadamente afetar as operações do negócio.
Baixa (1)	O papel ou parte terceira identificada tem acesso limitado aos ativos de informação classificados como públicos. Uma quebra de segurança por indivíduos a quem o papel está atribuído irá afetar insignificantemente as operações de negócio.	O papel ou parte terceira identificada tem privilégio limitado para mudar ativos de informação classificados como 'internos' ou 'públicos' e o seu trabalho é supervisionado. Uma quebra de segurança por indivíduos a quem o papel está atribuído irá afetar insignificantemente as operações de negócio.	Indisponibilidade do indivíduo a quem o papel está atribuído irá afetar insignificativamente as operações de negócio.

Tabela 22. Critérios de avaliação usados nos ativos humanos

Das tabelas acima podemos chegar à conclusão que os valores dos níveis de confidencialidade, integridade e disponibilidade são tomados como os seguintes:

Alto	3
Médio	2
Baixo	1

Tabela 23. Valores dos níveis de confidencialidade, integridade e disponibilidade

Com as tabelas acima podemos construir a seguinte matriz de avaliação dos ativos:

CIA Matrix

	Confidencialidade	Baixo			Médio			Alto		
	Integridade	Baixo	Médio	Alto	Baixo	Médio	Alto	Baixo	Médio	Alto
Disponibilidade	Baixo	3	4	5	4	5	6	5	6	7
	Médio	4	5	6	5	6	7	6	7	8
	Alto	5	6	7	6	7	8	7	8	9

Tabela 24. Matriz CIA

Através da Tabela 24, consegue-se para cada ativo obter o valor respetivo tendo em consideração a confidencialidade, disponibilidade e integridade. O valor do ativo é obtido através da soma dos valores de cada um dos princípios de segurança:

Valor do ativo = Confidencialidade + Integridade + Disponibilidade

No fim desta etapa, pretende-se que esteja construída uma tabela, por exemplo, em *Excel* onde se possa encontrar os ativos que de alguma forma interagem com a aplicação ou sistema em estudo. Será possível ver a que categoria o ativo pertence e qual o seu valor. Deve-se, caso seja necessário, justificar o valor atribuído ao ativo.

Este processo torna mais fácil decidir quais os ativos que devem ser protegidos.

7. Identificação das ameaças

Tipo	Ameaças
Dano físico	Partículas em suspensão / pó Ataque à bomba Danos causados nas linhas/cabos de comunicação Destruição de equipamento ou media Deterioração de equipamentos com informação Desastre causado por humanos Corrosão, congelamento

Dano físico	Contaminação ambiental (e outras formas de desastres naturais ou causados por humanos) Fogo Exposição à luz Poluição Flutuação de tensão Ataques terroristas Vandalismo Danos causados por água
Eventos naturais	Desastre (natural) Tremor de terra Temperatura e humidade extremas Inundação Furacão Relâmpago
Perda de serviços essenciais	Falha no ar condicionado Falha no fornecimento de água Perda de eletricidade Perda de serviços Interrupção de processos e atividades de negócio Perda de serviços de suporte
Comprometimento de informação	Dano causado por uma parte terceira Danos resultantes de um *penetration test* Informação de fontes não seguras Destruição de registos Destruição de planos de negócio Divulgação de informação Divulgação de passwords Espionagem Falsificação de registos Espionagem industrial Perda de registos Código malicioso *Software* malicioso (vírus, *worms, Trojan horses*) Perda de integridade Deteção da posição Erro do utilizador Espionagem remota Roubo de equipamento Roubo de documentos Mudança não intencional de informação num sistema de informação Interceção de sinais de interferência comprometedores Recuperação de informação reciclada ou descartada Adulteração com *hardware* Adulteração com *software*
Falhas técnicas	Falha do equipamento Mau funcionamento do equipamento Erros na manutenção Falha dos serviços de comunicação Falha dos componentes da rede Falha de *hardware* Falha de segurança Erros de transmissão Falha do sistema Falha de *software* Erros de *software* Saturação do sistema de informação Incidentes de segurança da informação Ameaça à manutenção do sistema de informação Falha de *links* de comunicação Sobrecarga de tráfego Repudiação (serviços, transições, mensagens enviadas e recebidas) Erro pessoal de suporte operacional
	Acesso à rede de pessoas não autorizadas Chantagem Procura de informação proprietária

Ações não autorizadas	Comprometimento de ativos Comprometimento de segurança Comprometimento de informação confidencial Corrupção de informação Exploração económica Quebra de legislação e regulamentos Uso ilegal de *software* Desfalque Ocultação da identidade do colaborador Cópia fraudulenta de *software* Importação/exportação ilegal de software Processamento de informação ilegal Quebra de relações/obrigações contratuais Infiltração de comunicações Suborno através de informação Introdução de código não autorizado ou não testado Má utilização dos sistemas de informação (acidental ou deliberada) Má utilização de ferramentas de registo de atividades Intrusão na privacidade pessoal Má utilização de recursos e ativos Desvio ou interceção de mensagens Venda de informação pessoal Ausência de colaboradores chave Uso não autorizado de equipamento de armazenamento Acesso não autorizado às tabelas de registo de atividades Acesso não autorizado ás ferramentas de registo de atividades Acesso não autorizado ao sistema de informação Mudança não autorizada de registos Instalação não autorizada de *software* Modificação não autorizada dos registos de atividades Acesso físico não autorizado Uso não autorizado de materiais com direitos de autor Uso não autorizado de *software* Uso de cópias de software ou *software* contrafeito Violação dos direitos de propriedade intelectual Utilização de recursos de rede de forma não autorizada
Comprometimento de funções	Abuso de direitos Quebra da disponibilidade dos colaboradores Negação de ações Ação industrial Interferência Greve Dano intencional Forjamento de direitos

8. Análise dos controlos

É importante identificar os controlos existentes ou planeados. O processo de apreciação do risco poderá indicar se os controlos existentes não são suficientes e novos podem ser introduzidos para reduzir o risco para níveis aceitáveis. A saída final desta fase deve ser uma lista de todos os controlos existentes ou planeados.

9. Identificação das vulnerabilidades

A avaliação das vulnerabilidades é o processo de identificar fraquezas que podem ser exploradas por ameaças que causam dano aos ativos e ao negócio que eles suportam. Uma

vulnerabilidade identificada não irá causar, em si mesma, dano a menos que uma ameaça esteja presente para a explorar.

Nesta fase da apreciação do risco, deve-se usar a seguinte tabela de forma a tentar perceber quais são as vulnerabilidades que se podem encontrar associadas a cada ativo.

Categoria do ativo	**Vulnerabilidades que podem ser encontradas**	
Hardware	• *Interface* de utilizador complicada • Linhas *dial-up* • Eliminação e reutilização de *storage media* sem eliminar informação • Sensibilidade do equipamento a mudanças de tensão • Sensibilidade do equipamento humidade e contaminantes • Sensibilidade do equipamento à temperatura	• Manutenção inadequada ou instalação defeituosa • Substituição inadequada de equipamento antigo • Cópias de informação não controladas • *Storage* não protegida • Falta de esquemas de substituição de equipamentos periódicos
Software	• Não mudança das passwords por defeito • Falta de redundância • Falta de procedimentos de *backups* • Datas incorretas • Falta de validação de informação processada • Falta de *updates* para salvaguardar contra *software* malicioso, isto é, antivírus e *anti spam* • Testes insuficientes de *software* • Falta de documentação • Falta de encriptação em dispositivos móveis, por exemplo, portáteis, PDAs • Estabelecimento incorreto de parâmetros • Proteção inadequada de chaves criptográficas • *Backup* irregular ou inadequado • Segurança inadequada dos cabos • *Software* novo ou imaturo • Falha a produzir relatórios de gestão • Falha a aplicar *patches* • Pobre seleção de informação de teste • Habilitação de serviços desnecessários	• Falta de mecanismos de monitorização para detetar tentativas intrusão, isto é, em redes, *hosts*, aplicações e espaço físico • Falta de mudança de controlo efetiva • Falta de sistemas de identificação e autenticação • Falta de ou pobre implementação de registo de atividades • Cópia única • Especificações de *software* não clara ou incompleta para desenvolvedores • Não proteção das tabelas de passwords • Falta de filtros de *spam* em sistemas de email • Gestão de passwords pobre (passwords facilmente adivinháveis, armazenamento de passwords, frequência de mudança insuficiente) • Vulnerabilidades conhecidas de *software* • Alocação errada de direitos de acesso • Falta de proteção para equipamentos móveis • Não fazer *logout* aquando da saída do posto de trabalho
Rede	• Gestão inadequada de rede • Arquitetura insegura de rede • Falta de controlo sobre a entrada e saída de informação • Tráfico sensível não protegido • Falta de prova de envio e receção de mensagens • Falta de monitorização das redes a partir dos sistemas de intrusão	• Falta de identificação e autenticação da pessoa que envia ou recebe a mensagem • Transferir passwords em texto claro • Ligações de redes públicas desprotegidas • Falha de ponto único • Ponto de ligação de cabos pobre

Pessoal	• Falta de pessoal • Processos inadequados de recrutamento • Consciência de segurança inadequada • Separação de deveres inadequada • Supervisão inadequada dos colaboradores • Supervisão inadequada de vendedores • Treino inadequado de colaboradores • Falta de políticas para um uso correto dos meios de telecomunicação e de mensagens	• Não remoção dos direitos de acesso aquando da terminação do contrato • Muito poder numa só pessoa • Não controlo de downloads e uso de software • Uso não controlado dos sistemas de informação • Colaboradores não motivados • Não supervisão do trabalho de colaboradores externos e pessoal de limpeza
Site	• Localização numa área suscetível a desastres naturais • Uso descuidado ou inadequado de controlos de acesso físico a edifícios, quartos e escritórios.	• Rede de energia instável • Separação inadequada de instalações operacional e de teste • Controlo inadequado de acessos físicos
Organização	• Capacidade inadequada de gestão • Mudança inadequada de gestão • Classificação inadequada de informação • Resposta de manutenção do serviço inadequada • Falta de um processo formal para registo e eliminação de registo dos colaboradores • Falta de documentação interna • Falta de política para o uso de criptografia • Falta de relatórios onde se encontram os registos de atividades dos operadores e administradores • Falta de processos de identificação e apreciação do riscos • Falta de um processo formal de revisão de direitos de acesso • Falta de um procedimento formal para registar a supervisão de um ISMS • Falta de registo de atividades regulares (supervisão) • Os direitos dos colaboradores não são revistos regularmente • A não existência de um procedimento para devolver um ativo no fim do contrato • Falta ou uma política insuficiente de mesas limpas e ecrãs limpos • Não existência ou insuficiente política de controlo de acesso	• Falta de um processo disciplinar definido no caso do acontecimento de um incidente de segurança da informação • Falta de planos de continuidade • Falta de política de controlo de acesso • Falta de processos de mudança de controlos • Falta de mecanismos de monitorização estabelecidos para quebras de segurança • Falta de uma política para o uso do correio eletrónico • Falta de uma política formal para o uso de portáteis • Falta de responsabilidade de segurança da informação na descrição dos trabalhos • Falta de processos para introduzir software nos sistemas operativos • Falta de processos para reportar vulnerabilidades na segurança • Falta de procedimentos de monitorização de instalações de processamento de informação • Falta ou insuficiente *Service Level Agreement (SLA)* • Falta de procedimentos para classificar a manipulação de informação • Falta ou insuficientes disposições (relativo a segurança da informação) em contratos com clientes, colaboradores e partes terceira

10. Identificação das potenciais consequências

Critérios devem ser usados para avaliar as consequências possíveis que podem resultar da perda de confidencialidade, integridade, disponibilidade, não repúdio, responsabilidade, autenticidade, ou confiança dos ativos:

• Exploração económica • Roubo de informação • *Social engineering* • *Hacking* • *Spoofing* • Sabotagem do sistema • Intrusão na privacidade pessoal • *Bugs* do sistema • Interceção de informação • Abuso dos computadores • Guerra de informação • Crime virtual (*cyber stalking*) • Quebra de confidencialidade • Comprometimento do desempenho do negócio • Quebra da ordem pública • Interrupção do serviço: incapacidade de fornecer o serviço • Perda de confiança do cliente • Perda de credibilidade no sistema de informação interno • Perda de eficiência • Rutura de operações internas • Custos financeiros em casos de emergência ou reparação: em termos de pessoal, equipamento, estudos. • Processos judiciais e multas • Demissão	• Fraude e/ou roubo • Venda de informação pessoal • Entrada de informação falsificada ou corrompida • Penetração do sistema • Ataque ao sistema (*Denial-of-Service* distribuído) • Intrusão no sistema • Adulteração do sistema • Assalto a um colaborador • Chantagem • Violação de legislação e regulamentos • Perda financeira • Comprometimento de informação pessoal • Rutura de atividades de negócio • Dano na reputação • Perda de vantagem competitiva • Danos a material • Perda de liderança tecnológica • Ataque à vida privada do titular dos dados • Efeitos adversos sobre a aplicação da lei • Quebra de contratos • Enfraquecimento da capacidade de negociação • Crises industriais (greves) • Perda de bens/fundos/ativos • Crise de governação

11. Identificação dos riscos

Depois das fases em que se identifica as vulnerabilidades, ameaças e potências consequências, é possível através da junção da vulnerabilidade e da ameaça do ativo, identificar um risco associado a cada ativo. É desta etapa que saem os riscos que são identificados para cada ativo e são os pilares iniciais de onde nasce a tabela de análise do risco do ambiente em estudo.

12. Determinação da probabilidade

Uma ameaça tem o potencial de causar um impacto negativo na organização. Para todas as ameaças, a fonte da ameaça (quem/o que pode causar a ameaça) e o alvo da ameaça (quais ativos podem ser afetados) devem ser determinadas e a probabilidade da ocorrência (definida aqui como a probabilidade de um evento indesejado ocorrer no futuro) deve ser avaliada. Isto deve ter em consideração:

- A frequência da ameaça (com que frequência pode ocorrer, de acordo com a experiência, estatísticas, relatórios de ocorrência de incidentes);
- A motivação, as capacidades, recursos necessários e disponíveis para possíveis atacantes e a perceção de atração e vulnerabilidade dos ativos de um sistema de TI para o possível atacante;
- Fatores geográficos tais como a proximidade a indústrias químicas ou petrolíferas, a possibilidade de condições de tempo extremas e fatores que podem influenciar erros humanos e mau funcionamento de equipamento.

A cada um dos pares vulnerabilidade/ameaça terá que ser atribuído um valor de probabilidade, que se dividem em três níveis, de acordo com a Tabela 25.

Avaliação da Probabilidade	
	Critério
Alta (3)	Os controlos de segurança existentes são poucos ou ineficazes. Há grandes probabilidades de que esses incidentes ocorram no futuro.
Média (2)	Os controlos de segurança existentes são moderados e na maioria das situações forneceram o nível de proteção adequado. Novos incidentes são possíveis no futuro.
Baixa (1)	Os controlos de segurança existentes são fortes e até agora forneceram o nível de proteção adequado. Nenhum novo incidente é esperado no futuro.

Tabela 25. Critérios para a avaliação da probabilidade.

13. Análise do impacto

Vários pontos devem ser considerados para avaliar o potencial impacto. Estes incluem:

- Qual é o impacto potencial para o tratamento do paciente?
- Qual é o impacto para a entrega do serviço?
- Qual é o impacto para a reputação da organização?
- Qual é o impacto potencial na privacidade/legislação/regulamentos?
- Qual é o impacto potencial financeiro sobre a organização?

De novo terá que se atribuir a cada um dos pares vulnerabilidade/ameaça um valor relativo ao seu impacto, caso este par consiga ser explorado. Os valores atribuídos ao impacto têm de ser atribuídos de acordo com a Tabela 26.

Avaliação do Impacto	
	Critério
Crítico	Coloca em causa a interrupção de atividade por período superior a 24h ou a continuidade do negócio
Alto	Coloca em causa a interrupção de atividade por período não superior a 2 dias úteis, ou causa prejuízos financeiros ou de imagem graves.
Médio	Coloca em causa a interrupção de atividade por período não superior a 8 horas, ou causa prejuízos financeiros ou de imagem moderados.
Baixo	Coloca em causa a interrupção de atividade por período não superior a 4 horas, ou causa prejuízos financeiros ou de imagem reduzidos.
Negligenciável	Coloca em causa a interrupção de atividade por período não superior a 1 hora, ou não causa prejuízos financeiros nem de imagem.

Tabela 26. Critérios para a avaliação do impacto

14. Determinação do nível do risco

A combinação da probabilidade e o tamanho do impacto dá origem a vários níveis de risco. A decisão no nível do risco final deve ter em conta:

- O valor monetário real do ativo em risco;
- A probabilidade da ocorrência de ameaças que podem causar impacto potencial adverso no negócio;
- A facilidade de exploração de vulnerabilidades pelas ameaças identificadas;
- Quaisquer controlos existentes ou planeados que podem reduzir o risco.

Depois da atribuição dos valores da probabilidade e do impacto, é possível calcular o nível do risco. O cálculo do nível de risco segue a seguinte forma:

Nível do risco = Probabilidade x Impacto x Valor do Ativo

Níveis de Risco																
Probabilidade		Baixo					Médio					Alto				
Impacto		N	B	M	A	C	N	B	M	A	C	N	B	M	A	C
Valor do Ativo	3	3	6	9	12	15	6	12	18	24	30	9	18	27	36	45
	4	4	8	12	16	20	8	16	24	32	40	12	24	36	48	60
	5	5	10	15	20	25	10	20	30	40	50	15	30	45	60	75
	6	6	12	18	24	30	12	24	36	48	60	18	36	54	72	90
	7	7	14	21	28	35	14	28	42	56	70	21	42	63	84	105
	8	8	16	24	32	40	16	32	48	64	80	24	48	72	96	120
	9	9	18	27	36	45	18	36	54	72	90	27	54	81	108	135

Tabela 27. Cálculo do nível do risco

A confidencialidade, integridade e disponibilidade de um ativo são os princípios que devem ser mantidos a nível da segurança da informação. O risco é, portanto, a função do valor ou criticidade de um ativo, a probabilidade das vulnerabilidades dos sistemas que incorporam os ativos disponíveis serem exploradas por ameaças.

15. Recomendação dos controlos

O objetivo da recomendação de controlos é reduzir o nível de risco de um sistema de TI e a sua informação para um nível aceitável. Os seguintes fatores devem ser considerados na recomendação dos controlos e soluções alternativas para minimizar ou eliminar os riscos identificados.

Os controlos só deverão ser identificados se a vulnerabilidade identificada pode ser explorada pela ameaça correspondente. A escolha dos controlos deve-se basear nos riscos atuais dos ativos que têm algum valor para a organização.

16. Justificação dos controlos recomendados

Depois da recomendação dos controlos estar realizada, será necessário justificar à luz da organização e porquê de ela dever implementar esses controlos. Não se deve criar uma lista dos controlos implementados e dizer à organização que os tem de implementar, mas essa lista deve vir complementado com o porquê da justificação dos controlos, de forma a organização perceber, qual é o enquadramento presente em cada um e dessa forma priorizar a implementação dos controlos.

Deve-se agrupar dados de organizações ou entidades com que a organização se identifique, percebendo dessa forma todo o pensamento que levou à recomendação de

determinado controlo. Pode-se pensar que esta é uma etapa desnecessária, mas só trará vantagens à organização quando existir a tomada da decisão: que controlos implementar em primeiro lugar?

17. Documentação dos resultados

Quando todas as etapas anteriores estiverem concluídas é necessário que todos os resultados e conclusões sejam colocados num documento. Esta criação de documentos como fase final de uma apreciação do risco é benéfica, pois possibilitará comparar resultados, e quem sabe criar métricas baseadas nestes resultados de forma a permitir obter uma melhor perceção da saúde do sistema que se está a avaliar.

Deve-se atribuir a responsabilidade a um colaborador, para periodicamente conduzir um teste à segurança e uma apreciação do risco para assegurar que existe uma representação precisa e temporal das vulnerabilidades, ameaças, riscos e controlos para manter a informação dos pacientes protegida. Esta informação deve ser usada para assegurar que os controlos apropriados estão em lugar e que os riscos são documentados e mantidos num nível aceitável e possíveis de gerir.

Referências utilizadas na elaboração metodologia:

[1] *Guide to Information Security for the Health Care Sector*, eHealth Ontario, Information and Resources for Complex Organizations

[2] ISO/IEC 27005:2008, *Information technology – Security techniques – Information security risk management*

[3] *Matrices for Asset Valuation and Risk Analysis*, ISO 27001 Implementer's Forum

[4] *Guide for Conducting Risk Assessments*, Information Security, NIST Special Publication 800-30 Revision 1

Apêndice 3 – Métricas Desenvolvidas

Neste apêndice podemos encontrar as métricas geradas através da metodologia descrita no capítulo 3 e de acordo com os resultados da escolha das métricas para o modelo, que estão expostas no capítulo 4, na seção 4.3.

Identificação do Modelo de Medição	
Nome do Modelo de Medição	Segregação de deveres ao nível dos acessos à informação.
Identificador Numérico	Específica da organização.
Propósito do Modelo de Medição	Mostrar a existência, a extensão e a qualidade dos controlos implementados que permitem a segregação de deveres ao nível de acesso à informação existente.
Objetivo do Controlo/Processo	A.6.1 [27001:2013] *Internal organization* *To establish a management framework to initiate and control the implementation and operation of information security within the organization.*
Controlo(1)/Processo(1)	A.6.1.2 [27001:2013] *Segregation of duties* *Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.*
Objetos de Medição e Atributos	
Objeto de Medição	Tabelas de ativos e seus responsáveis.
Atributo	Colaboradores responsáveis por ativos.
Especificação da Métrica Base	
Métrica Base	1. Número de colaboradores responsáveis por ativos que não têm registo de atividades (*logging*). 2. Número de colaboradores responsáveis por ativos.
Método de Medição	1. Contar o número de colaboradores responsáveis por ativos que não têm registo de atividades. 2. Contar o número de colaboradores responsáveis por ativos.
Tipo do Método de Medição	1. Objetivo 2. Objetivo
Escala	1. Inteiros de zero até infinito. 2. Inteiros de zero até infinito.
Tipo de Escala	1. Ordinal 2. Ordinal
Unidade de Medição	1. Colaboradores 2. Colaboradores
Especificação da Métrica Derivada	
Métrica derivada	Percentagem (%) de colaboradores que podem aceder, alterar ou destruir informação sem serem detetados.
Função de Medição	(Número de colaboradores responsáveis por ativos que não têm registo de atividades) / (Número de colaboradores responsáveis por ativos) * 100
Especificação do Indicador	
Indicador	Gráfico de colunas representando a percentagem de colaboradores que podem aceder, alterar ou destruir informação sem serem detetados por cada ano em que este controlo é avaliado.
Modelo Analítico	Colunas que ultrapassem o valor de 10% devem aparecer a vermelho. Abaixo ou igual a 10% deve aparecer a amarelo.

Especificação do Modelo de Decisão	
Critérios de Decisão	Colunas a vermelho – devem ser tomadas decisões imediatas para baixar este valor. Colunas a amarelo – avaliar os casos onde não existe separação de deveres e identificar aqueles onde a organização poderia tomar ações.
Resultados de Medição	
Interpretação do Indicador	Valores acima de 10% devem fazer com que se tome medidas para que a tendência volte a estar nesse valor ou descer. Esta percentagem deve sempre tender para zero pois não deve existir nenhuma situação onde um colaborador possa aceder, alterar ou destruir informação que no setor da saúde é extremamente importante. Se não for possível tornar a baixar o valor abaixo de 10% deve-se justificar a não tomada de ações. As colunas a amarelo representam casos de não separação de deveres que se devem ter em consideração. A organização deve estar ciente que é necessário não deixar que este valor aumente, chegando a ficar acima dos 10%.
Formatos de Apresentação	Gráfico de colunas que retrata a tendência ao longo dos anos com um sumário das descobertas, ações tomadas ou não consoante os valores obtidos, e justificando a tomada ou não de ações. O relatório deve também justificar sempre a percentagem existente mesmo que abaixo de 10%.
Partes Interessadas	
Cliente para a Medição	Gestor responsável pelo SGSI.
Revisor para a Medição	Gestor de segurança.
Proprietário da Informação	Gestor de segurança.
Compilador da Informação	Gestor de segurança.
Comunicador da Informação	Gestor responsável pelo SGSI.
Frequência/Período	
Frequência da Recolha de Dados	Anual.
Frequência da Análise de Dados	Anual.
Frequência de Apresentação dos Resultados d Medição	Anual.
Revisão da Medição	Rever e atualizar a cada dois anos.
Período de Medição	Aplicável por dois anos.

Tabela 28. Métrica: Percentagem (%) de colaboradores que podem aceder, alterar ou destruir informação sem serem detetados.

Identificação do Modelo de Medição	
Nome do Modelo de Medição	Credenciais distintas para acesso a aplicações.
Identificador Numérico	Específico da organização
Propósito do Modelo de Medição	Verificar a existência da problemática que muitos utilizadores podem encontrar se existirem passwords distintas para cada uma das aplicações que podem necessitar no seu dia-a-dia. A existência de demasiadas passwords pode levar a que coloquem as passwords iguais ou sejam extremamente fracas/fáceis de adivinhar.
Objetivo do Controlo/Processo	A.9.3 [27001:2013] *User responsibilities* *To make users accountable for safeguarding their authentication information.*
Controlo(1)/Processo(1)	A.9.3.1 [27001:2013] *Use of secret authentication information* *User shall be required to follow the organization's practices in the use of secret authentication information.*
Objeto de Medição e Atributos	
Objeto de Medição	Tabelas de passwords de cada aplicação.
Atributo	Passwords das aplicações.
Especificação da Métrica Base (1)	
Métrica Base	1. Número de grupos de profissionais existentes no centro hospitalar. 2. Número de passwords diferentes que cada grupo necessita.
Método de Medição	1. Correr uma *query* para saber o número de grupos de profissionais que existem no centro hospitalar. 2. Correr uma *query* para saber o número de passwords diferentes que cada grupo necessita para trabalhar.
Tipo do Método de Medição	1. Objetivo. 2. Objetivo.
Escala	1. Inteiros de zero a infinito. 2. Inteiros de zero a infinito.
Tipo da Escala	1. Ordinal. 2. Ordinal.
Unidade de Medição	1. Grupos de profissionais de saúde. 2. Passwords.
Especificação da Métrica Derivada	
Métrica Derivada	Média de credenciais diferentes que um utilizador poderá necessitar no seu dia de trabalho.
Função da Medição	Somatório do (Número de passwords diferentes que cada grupo necessita para trabalhar) / (Número de grupos de profissionais que existem no centro hospitalar)
Especificação do Indicador	
Indicador	Tendência do número de credenciais distintas que um profissional de saúde precisa num dia de trabalho.
Modelo Analítico	Comparar com medições anteriores.
Especificação do Critério de Decisão	

Critério de Decisão	Se a tendência for descendente, a organização está no caminho certo. Se a tendência for ascendente será necessário avaliar o porquê dessa situação.
Resultados da Medição	
Interpretação do Indicador	Se a tendência se observar descendente a organização está no caminho certo, permitindo que os profissionais de saúde não tenham de memorizar tantas passwords, diminuindo assim o risco de cometerem ações que coloquem em risco a organização e a entrada não autorizada nos seus sistemas Se a tendência se observar ascendente, deve-se levar a cabo uma investigação de forma a perceber o porquê do número de credenciais estar a aumentar, colocando em maior risco a organização. Deve-se estudar a possibilidade de eliminar algumas dessas passwords, de forma a melhorar o dia-a-dia de todos os profissionais de saúde que fazem parte do centro hospitalar.
Formato de Apresentação	Deverá ser apresentado um gráfico de linhas que mostra a evolução quanto ao número médio de credenciais que um profissional de saúde precisa no seu dia-a-dia.
Partes Interessadas	
Cliente para a Medição	Gestor responsável pelo SGSI.
Revisor para a Medição	Gestor de segurança.
Proprietário da Informação	Gestor de segurança.
Compilador da Informação	Gestor de segurança.
Comunicador da Informação	Gestor responsável pelo SGSI.
Frequência/Período	
Frequência da Recolha dos Dados	Anual.
Frequência da Análise dos Dados	Anual.
Frequência de Apresentação dos Resultados d Medição	De dois em dois anos.
Revisão da Medição	De dois em dois anos.
Período de Medição	Anualmente.

Tabela 29. Número médio de credenciais distintas por utilizador.

Identificação do Modelo de Medição	
Nome do Modelo de Medição	Contas não correlacionadas.
Identificador Numérico	Específico da organização
Propósito do Modelo de Medição	Verificação da existência de contas não correlacionadas (que não estão a ser usadas), podendo estas ser usadas para atacar a organização.
Objetivo do Controlo/Processo	A.9.2 [27001:2013] *User access management* *To ensure authorized user access and to prevent unauthorized access to systems and services.*
Controlo(1)/Processo(1)	A.9.2.6 [27001:2013*] Removal or adjustment of access rights* *The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.*
Objeto de Medição e Atributos	
Objeto de Medição	Aplicações.
Atributo	Contas existentes em cada aplicação.
Especificação da Métrica Base (1)	
Métrica Base	1. Número de contas por cada aplicação. 2. Número de contas por cada aplicação que não estão correlacionadas com nenhum colaborador.
Método de Medição	1. Correr uma *query* para saber o número de contas por cada aplicação. 2. Correr uma *query* para saber o número de contas por cada aplicação que não estão correlacionadas com nenhum colaborador.
Tipo do Método de Medição	1. Objetivo. 2. Objetivo.
Escala	1. Inteiros de zero até ao infinito. 2. Inteiros de zero até ao infinito.
Tipo da Escala	1. Ordinal. 2. Ordinal.
Unidade de Medição	1. Contas da aplicação em análise. 2. Contas da aplicação em análise.
Especificação da Métrica Derivada	
Métrica Derivada	Percentagem (%) de contas não correlacionadas por aplicação.
Função da Medição	(Número de contas não correlacionadas da aplicação) / (Número de contas da aplicação) * 100
Especificação do Indicador	
Indicador	1. Gráfico de barras que no eixo horizontal apresenta as aplicações presentes no centro hospitalar e no eixo horizontal, valores de 0% a 100%. 2. Tendência na eliminação de contas aquando da saída de colaboradores da organização.
Modelo Analítico	As barras com mais de 10% devem aparecer a vermelho. As barras menores ou iguais a 10% devem aparecer a amarelo.
Especificação do Critério de Decisão	
Critério de Decisão	As barras a vermelho requerem, além de intervenção imediata da eliminação dessas contas,

	que a pessoa acima do responsável pela aplicação determine as razões da existência de tantas contas não correlacionadas. As barras amarelas indicam que os responsáveis por essas aplicações devem intervir imediatamente nessas contas.
Resultados da Medição	
Interpretação do Indicador	É objetivo das organizações não possuir contas não correlacionadas, mostrando que o processo de revocação dos acessos dos colaboradores que deixam o centro hospitalar é realizado com sucesso. Quando se verifica a existência de percentagens menores ou iguais a 10% das contas da aplicação, pode-se explicar isso como um erro que pode ter ocorrido quer da parte do responsável como da parte da aplicação que trata destes processos. De qualquer forma deve-se analisar essas contas e remove-las, caso não se faça a remoção deve ficar documentado o porquê dessa ação. Quando se verifica valores de percentagem maiores que 10%, deve-se interpretar essa situação como a possibilidade de negligência do administrador, devendo-se levar a cabo uma análise para perceber o porquê dessa situação e mais uma vez analisar essas contas e removê-las.
Formato de Apresentação	Deverá ser apresentado um gráfico de linhas que mostra a evolução para cada aplicação da tendência sobre o número de contas não correlacionadas, durante o ano de medição.
Partes Interessadas	
Cliente para a Medição	Gestor responsável pelo SGSI.
Revisor para a Medição	Gestor de segurança.
Proprietário da Informação	Gestor de segurança.
Compilador da Informação	Gestor de segurança.
Comunicador da Informação	Gestores responsáveis pelo SGSI.
Frequência/Período	
Frequência da Recolha dos Dados	Mensal.
Frequência da Análise dos Dados	Mensal.
Frequência de Apresentação dos Resultados d Medição	Anualmente.
Revisão da Medição	Anualmente.
Período de Medição	Anual.

Tabela 30. Percentagem (%) de contas não correlacionadas por aplicação.

Identificação do Modelo de Medição	
Nome do Modelo de Medição	Registo de atividades nas aplicações.
Identificador Numérico	Específico da organização
Propósito do Modelo de Medição	Perceber em que ponto a organização está em relação ao registo de atividades dentro das aplicações.
Objetivo do Controlo/Processo	A.12.4 [27001: 2013] *Logging and Monitoring* *To record events and generate evidence.*
Controlo(1)/Processo(1)	A.12.4.1[27001: 2013] *Event logging* *Event logs recording user activities, expectations, faults and information security events shall be produced, kept and regularly reviewed.*
Objeto de Medição e Atributos	
Objeto de Medição	Aplicações.
Atributo	Característica de registo de atividades.
Especificação da Métrica Base (1)	
Métrica Base	1. Número de aplicações existentes. 2. Número de aplicações que têm registo de atividade: entrada, operações realizadas e saída.
Método de Medição	1. Contar o número de aplicações existentes. 2. Contar o número de aplicações com os registos de atividades descritos.
Tipo do Método de Medição	1. Objetivo. 2. Objetivo.
Escala	1. Inteiros de zero a infinito. 2. Inteiros de zero a infinito.
Tipo da Escala	1. Ordinal. 2. Ordinal.
Unidade de Medição	1. Aplicações. 2. Aplicações.
Especificação da Métrica Derivada	
Métrica Derivada	Percentagem (%) de aplicações com registo de atividades: entradas, operações realizadas e saídas.
Função da Medição	(Número de aplicações com registo de atividades) / (Número de aplicações existentes) * 100
Especificação do Indicador	
Indicador	Tendência da percentagem de aplicações com registo de atividades.
Modelo Analítico	Comparar das percentagens obtidas em anteriores medições.
Especificação do Critério de Decisão	
Critério de Decisão	A linha que representa a tendência deve-se manter constante ou baixar em relação às medições anteriores.
Resultados da Medição	
Interpretação do Indicador	Se a tendência da percentagem estiver a subir nada deve ser feito. Se a tendência da percentagem estiver a descer tem que se avaliar o porquê dessa tendência. Se a linha da tendência de a percentagem diminuir, pode não querer dizer que os números de aplicações com encriptação diminuíram, mas que o número de aplicações aumentou na organização, não tendo sido consideradas as caraterísticas de encriptação

	aquando da sua aquisição. Dessa forma é necessário que a organização perceba o porquê desta característica não ter sido considerada. Isto é importante pois pode colocar a organização em incumprimento de regulamentos e leis existentes.
Formato de Apresentação	Gráfico de linhas unindo as várias percentagens resultantes das várias medições anteriores.
Partes Interessadas	
Cliente para a Medição	Gestor responsável pelo SGSI.
Revisor para a Medição	Gestor de segurança.
Proprietário da Informação	Gestor de segurança.
Compilador da Informação	Gestor de segurança.
Comunicador da Informação	Gestor responsável pelo SGSI.
Frequência/Período	
Frequência da Recolha dos Dados	Anual.
Frequência da Análise dos Dados	Anual.
Frequência de Apresentação dos Resultados d Medição	De dois em dois anos.
Revisão da Medição	De dois em dois anos.
Período de Medição	Anual.

Tabela 31. Percentagem (%) de aplicações com registo de atividades: entrada na aplicação e operações realizadas.

Identificação do Modelo de Medição	
Nome do Modelo de Medição	Controlo do fluxo de informação.
Identificador Numérico	Específico da organização
Propósito do Modelo de Medição	Entender se há na organização aplicações que permitem a não possibilidade do controlo do fluxo de informação.
Objetivo do Controlo/Processo	A.18.1 [27001: 2013] *Compliance with legal and contractual requirements* *To avoid breaches of legal, statuary, regulatory or contractual obligations related to information security and of any security requirements.*
Controlo(1)/Processo(1)	A.18.1.4 [27001: 2013] *Privacy and protection of personally identifiable information* *Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.*
Objeto de Medição e Atributos	
Objeto de Medição	Aplicações existentes na organização.
Atributo	Existência de controlos de fluxo de informação.
Especificação da Métrica Base (1)	
Métrica Base	1. Número de aplicações existentes. 2. Número de aplicações que possibilitam cópias de informação.
Método de Medição	1. Contar o número de aplicações existentes. 2. Contar o número de aplicações que possibilitam cópias de informação.
Tipo do Método de Medição	1. Objetivo. 2. Objetivo.
Escala	1. Inteiros de zero a infinito. 2. Inteiros de zero a infinito.
Tipo da Escala	1. Ordinal. 2. Ordinal.
Unidade de Medição	1. Aplicações. 2. Aplicações.
Especificação da Métrica Derivada	
Métrica Derivada	Percentagem (%) de aplicações que possibilitam cópias de informação.
Função da Medição	(Número de aplicações que possibilitam cópias de informação) / (Número de aplicações existentes) * 100
Especificação do Indicador	
Indicador	Tendência ao longo do tempo da percentagem de aplicações que possibilitam cópias de informação, restringindo assim o fluxo de informação da organização.
Modelo Analítico	Comparar das percentagens obtidas em medições anteriores.
Especificação do Critério de Decisão	
Critério de Decisão	Se a tendência descer, ou seja, a percentagem de aplicações que possibilitam o controlo de informação na organização aumentar, não se deve fazer nenhuma ação. Caso a tendência continuar constante ou aumentar, deve-se analisar o porquê dessa diminuição.

Resultados da Medição	
Interpretação do Indicador	Uma interpretação que se deve fazer da tendência, que mostra o percurso desta característica nas aplicações, é que se a tendência aumentar ou se manter constante sem que o número de aplicações aumenta, deve-se analisar o que aconteceu para que esta característica tenha desaparecido de alguma das aplicações ou por que razão ao longo dos anos nada está a ser feito quanto ao risco que representa a não implementação de controlos de fluxo de informação. Caso a tendência aumente, porque o número de aplicações aumentou, deve-se perceber porque é que na aquisição de novas aplicações não foi considerada esta característica. Caso a tendência se mostre descendente a organização já a trabalhar no sentido de um maior controlo de segurança da informação.
Formato de Apresentação	Gráfico de linhas unindo as várias percentagens resultantes das várias medições anteriores.
Partes Interessadas	
Cliente para a Medição	Gestor responsável pelo SGSI.
Revisor para a Medição	Gestor de segurança.
Proprietário da Informação	Gestor de segurança.
Compilador da Informação	Gestor de segurança.
Comunicador da Informação	Gestor responsável pelo SGSI.
Frequência/Período	
Frequência da Recolha dos Dados	Anual.
Frequência da Análise dos Dados	Anual.
Frequência de Apresentação dos Resultados d Medição	Anualmente.
Revisão da Medição	Anualmente.
Período de Medição	Anual.

Tabela 32. Percentagem (%) de aplicações que impossibilitam cópias de segurança.

Identificação do Modelo de Medição	
Nome do Modelo de Medição	Contas partilhadas
Identificador Numérico	Específico da organização
Propósito do Modelo de Medição	Entender se existe o problema de contas partilhadas, o que permite que as ações dessas contas sejam realizadas sem se perceber quem as realizou.
Objetivo do Controlo/Processo	A.9.2 [27001: 2013] *User access management* *To ensure authorized user access and to prevent unauthorized access to systems and services.*
Controlo(1)/Processo(1)	A.9.2.3 [27001: 2013] *Management of privileged access rights* *The allocation and use of privileged access rights shall be restricted and controlled.*
Objeto de Medição e Atributos	
Objeto de Medição	Tabela agregadora de passwords das aplicações.
Atributo	Passwords
Especificação da Métrica Base (1)	
Métrica Base	1. Número completo de passwords; 2. Número de passwords que pertencem a grupos que são partilhados por vários colaboradores
Método de Medição	1. Correr uma *query* para saber o número completo de passwords que existem. 2. Correr uma *query* para saber o número de passwords que pertencem a grupos que são partilhados por vários colaboradores.
Tipo do Método de Medição	1. Objetivo. 2. Objetivo.
Escala	1. Inteiros de zero a infinito. 2. Inteiros de zero a infinito.
Tipo da Escala	1. Ordinal. 2. Ordinal.
Unidade de Medição	1. Palavras-passe. 2. Palavras-passe.
Especificação da Métrica Derivada	
Métrica Derivada	Percentagem (%) de palavras-passe que são partilhadas por vários colaboradores.
Função da Medição	(Número de passwords que pertencem a grupos que são partilhados por vários colaboradores) / (Número completo de passwords que existem) * 100
Especificação do Indicador	
Indicador	Tendência ao longo do tempo da percentagem de palavras-passes que são partilhadas por grupos de colaboradores.
Modelo Analítico	Comparar das percentagens obtidas em medições anteriores.
Especificação do Critério de Decisão	
Critério de Decisão	Se a tendência diminuir a organização está no bom caminho, e não é necessária intervenção imediata. Caso se verifique o contrário ou se mantiver a mesma tendência deve-se proceder à análise dessas situações e alterar essas situações.
Resultados da Medição	
Interpretação do Indicador	A diminuição da tendência ao longo das várias medições mostrará que a organização não está a

	dar continuidade à mesma ação e está a melhorar a sua atitude quanto às contas partilhadas. Caso a tendência se mantenha ou aumente a organização terá que rever o porquê da situação se estar a repetir. A existência de contas partilhadas é extremamente perigosa, pois mesmo que as aplicações tenham registo de atividades estas não serviriam de muito se algum problema acontece.
Formato de Apresentação	Gráfico de linhas unindo as várias percentagens resultantes das várias medições anteriores.
Partes Interessadas	
Cliente para a Medição	Gestor responsável pelo SGSI.
Revisor para a Medição	Gestor de segurança.
Proprietário da Informação	Gestor de segurança.
'Recolhedor' da Informação	Gestor de segurança.
Comunicador da Informação	Gestor responsável pelo SGSI.
Frequência/Período	
Frequência da Recolha dos Dados	Semestral.
Frequência da Análise dos Dados	Semestral.
Frequência de Apresentação dos Resultados d Medição	Anualmente.
Revisão da Medição	Anualmente.
Período de Medição	Anual.

Tabela 33. Percentagem (%) de contas partilhados.

Identificação do Modelo de Medição	
Nome do Modelo de Medição	Controlos de *session time-out*.
Identificador Numérico	Específico da organização
Propósito do Modelo de Medição	Perceber se este é uma preocupação que a organização tem, e se o esforço que têm vindo a fazer é no sentido de aumentar os controlos de *session time-out*.
Objetivo do Controlo/Processo	A.11.2 [27001: 2013] *Equipment* *To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.*
Controlo(1)/Processo(1)	A.11.2.1 [27001: 2013] *Equipment siting and protection* *Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.*
Objeto de Medição e Atributos	
Objeto de Medição	Tabela agregadora das características das aplicações.
Atributo	Controlos de *session time-out*.
Especificação da Métrica Base (1)	
Métrica Base	1. Número de aplicações do centro hospitalar; 2. Número de aplicações com *session time-out*
Método de Medição	1. Contar o número de aplicações existentes na organização. 2. Contar o número de aplicações com controlos de *session time-out*.
Tipo do Método de Medição	1. Objetivo. 2. Objetivo.
Escala	1. Inteiros de zero a infinito. 2. Inteiros de zero a infinito.
Tipo da Escala	1. Ordinal. 2. Ordinal.
Unidade de Medição	1. Aplicações. 2. Aplicações.
Especificação da Métrica Derivada	
Métrica Derivada	Percentagem (%) de aplicações com controlos de *session time-out*.
Função da Medição	(Número de aplicações com controlo de *session time-out*) / (Número de aplicações existentes) * 100
Especificação do Indicador	
Indicador	Tendência ao longo do tempo da percentagem de aplicações com controlos de *session time-out*.
Modelo Analítico	Comparar das percentagens obtidas em medições anteriores.
Especificação do Critério de Decisão	
Critério de Decisão	A tendência da percentagem deve-se manter acima dos 80%, caso desça abaixo desse valor deve-se levar a cabo uma avaliação para colocar a tendência nesse valor.
Resultados da Medição	
Interpretação do Indicador	Este indicador dará a perceção de como a implementação destes controlos nas aplicações está a acontecer. O valor de 80% de aplicações com

	a implementação destes controlos, é um valor razoável já que não é pedido os 100%, sobra ali uns 20% para a equipa de segurança puder estar atenta a esses casos. Mas sempre que a tendência descer para valores abaixo dos 80%, esta torna-se um indicador de risco e a organização deve analisar as aplicações que não têm estes controlos e estudar a viabilidade de os implementar.
Formato de Apresentação	Gráfico de linhas unindo as várias percentagens resultantes das várias medições anteriores.
Partes Interessadas	
Cliente para a Medição	Gestor responsável pelo SGSI.
Revisor para a Medição	Gestor de segurança.
Proprietário da Informação	Gestor de segurança.
Compilador da Informação	Gestor de segurança.
Comunicador da Informação	Gestor responsável pelo SGSI.
Frequência/Período	
Frequência da Recolha dos Dados	Anual.
Frequência da Análise dos Dados	Anual.
Frequência de Apresentação dos Resultados d Medição	Anualmente.
Revisão da Medição	Anualmente.
Período de Medição	Anual.

Tabela 34. Percentagem (%) de aplicações com controlos de session time-out.

Identificação do Modelo de Medição	
Nome do Modelo de Medição	Encriptação de informação.
Identificador Numérico	Específico da organização
Propósito do Modelo de Medição	Perceber a extensão da encriptação de dados na organização.
Objetivo do Controlo/Processo	A.18.1 [27001: 2013] *Compliance with legal and contractual requirements* *To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.*
Controlo(1)/Processo(1)	A.18.1.4 [27001: 2013] *Privacy and protection of personally identifiable information* *Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation when applicable.*
Objeto de Medição e Atributos	
Objeto de Medição	Aplicações do centro hospitalar.
Atributo	Implementações de encriptação.
Especificação da Métrica Base (1)	
Métrica Base	1. Número de aplicações contendo informação confidencial de pacientes. 2. Número de aplicações que contendo informação confidencial de pacientes tem encriptação de dados.
Método de Medição	1. Contar o número de aplicações contendo informação confidencial de pacientes. 2. Contar o número de aplicações que contendo informação confidencial de pacientes tem encriptação de dados.
Tipo do Método de Medição	1. Objetivo. 2. Objetivo.
Escala	1. Inteiros de zero a infinito. 2. Inteiros de zero a infinito.
Tipo da Escala	1. Ordinal. 2. Ordinal.
Unidade de Medição	1. Aplicações. 2. Aplicações.
Especificação da Métrica Derivada	
Métrica Derivada	Percentagem (%) de aplicações que contendo informação confidencial de pacientes tem os seus dados encriptados.
Função da Medição	(Número de aplicações que contendo informação confidencial de pacientes, têm encriptação) / (Número de aplicações que contêm informação de pacientes) *100
Especificação do Indicador	
Indicador	Um gráfico de linhas representando a tendência na percentagem de aplicações com encriptação de dados ao longo do tempo em que foram feitas medições.
Modelo Analítico	Comparar das percentagens obtidas em medições anteriores.
Especificação do Critério de Decisão	
Critério de Decisão	Se a tendência se apresentar como ascendente, nada deve ser feito. Caso a tendência se mostrar

	descendente, a organização tem de examinar a performance negativa.
Resultados da Medição	
Interpretação do Indicador	Uma tendência ascendente em direção aos 100% é desejável, e se for esse o caso a organização está no caminho certo, podendo-se interpretar que além de incluírem essa característica nas aplicações existentes, também o consideram aquando da aquisição de novas aplicações. Caso a tendência se mostrar descendente, pode ser devido à inclusão de mais aplicações na organização, mas isto não deve servir como entrave, pois a organização deveria ter cuidado em adquirir aplicações que já incluíssem esta característica. Se a tendência se mantiver constante deve-se analisar a razão da organização não considerar a implementação de encriptação nas aplicações já existentes.
Formato de Apresentação	Gráfico de linhas unindo as várias percentagens resultantes das várias medições anteriores.
Partes Interessadas	
Cliente para a Medição	Gestor responsável pelo SGSI.
Revisor para a Medição	Gestor de segurança.
Proprietário da Informação	Gestor de segurança.
Compilador da Informação	Gestor de segurança.
Comunicador da Informação	Gestor responsável pelo SGSI.
Frequência/Período	
Frequência da Recolha dos Dados	Anual.
Frequência da Análise dos Dados	Anual.
Frequência de Apresentação dos Resultados d Medição	De dois em dois anos.
Revisão da Medição	De dois em dois anos.
Período de Medição	Anual.

Tabela 35. Percentagem (%) de aplicações que contendo informação confidencial de pacientes têm os seus dados encriptados.

Identificação do Modelo de Medição	
Nome do Modelo de Medição	*Password reset.*
Identificador Numérico	Específico da organização
Propósito do Modelo de Medição	Perceber o volume de *password reset* pode servir como dados que justifiquem um investimento na área de IAM. Esta medição pode demonstrar que os colaboradores têm preocupação com a segurança dos seus sistemas, pois mudam as passwords inicialmente atribuídas, mas que com o sistema de autenticação para entrar nas aplicações não é eficaz. A necessidade de se lembrar de todas as passwords é um problema que deve ser resolvido.
Objetivo do Controlo/Processo	A.9.4 [27001: 2013] *System and application access control* *To prevent unauthorized access to systems and applications.*
Controlo(1)/Processo(1)	A.9.4.3 [27001: 2013] *Password management system* *Password management systems shall be interactive and shall ensure quality passwords.*
Objeto de Medição e Atributos	
Objeto de Medição	Tabelas de passwords das aplicações.
Atributo	Passwords.
Especificação da Métrica Base (1)	
Métrica Base	1. Número total de passwords existentes em todas as aplicações da organização. 2. Número de passwords a que foi necessário fazer *reset*.
Método de Medição	1. Correr uma *query* para saber o número total de passwords existentes em todas as aplicações da organização. 2. Correr uma *query*, a nível da aplicação gestão de identidades, para saber o número de passwords a que foi necessário fazer *reset*.
Tipo do Método de Medição	1. Objetiva. 2. Objetiva.
Escala	1. Inteiros de zero a infinito. 2. Inteiros de zero a infinito.
Tipo da Escala	1. Ordinal. 2. Ordinal.
Unidade de Medição	1. Passwords. 2. Passwords.
Especificação da Métrica Derivada	
Métrica Derivada	Percentagem (%) de passwords que foi necessário fazer *reset*.
Função da Medição	(Número de passwords a que foi necessário fazer *reset*) / (Número de passwords total existente na organização) * 100
Especificação do Indicador	
Indicador	Tendência ao longo do tempo da percentagem de passwords a que foi necessário fazer *reset*.
Modelo Analítico	Comparar das percentagens obtidas em medições anteriores.
Especificação do Critério de Decisão	

Critério de Decisão	Se a tendência for ascendente, devia-se avaliar o porquê de isto estar a acontecer e estudar uma solução para o problema. Se a tendência for descendente, a organização não terá necessidade de se preocupar muito com esta situação.
Resultados da Medição	
Interpretação do Indicador	Esta tendência será capaz de representar a evolução quanto ao número de passwords *reset* ao longo de um ano e depois comparar com medições anteriores. Com uma tendência constante ou descendente a organização não precisa de se focar muito neste tipo de problema. Os profissionais de saúde já não estarão a perder muito tempo com o *reset* de passwords e os restantes profissionais de saúde já não estarão a encontrar grandes problemas em termos de memorizar as diferentes passwords. Caso a tendência seja ascendente, a organização deverá avaliar o porquê desta situação estar a acontecer e talvez estudar a possibilidade de implementar uma solução capaz de minimizar este problema, quer da parte dos técnicos da área informática quer dos restantes profissionais de saúde.
Formato de Apresentação	Gráfico de linhas unindo as várias percentagens resultantes das várias medições anteriores.
Partes Interessadas	
Cliente para a Medição	Gestor responsável pelo SGSI.
Revisor para a Medição	Gestor de segurança.
Proprietário da Informação	Gestor de segurança.
Compilador da Informação	Gestor de segurança.
Comunicador da Informação	Gestor responsável pelo SGSI.
Frequência/Período	
Frequência da Recolha dos Dados	Semestral.
Frequência da Análise dos Dados	Semestral.
Frequência de Apresentação dos Resultados d Medição	Anualmente
Revisão da Medição	Anual.
Período de Medição	Anual.

Tabela 36. Percentagem de passwords a que foi necessário fazer reset.

Anexo 1 – Modelo para a Construção de Métricas Apresentado pela ISO/IEC 27004

Measurement Construct Identification	
Measurement Construct Name	
Numerical Identifier	
Purpose of Measurement Construct	
Control/Process Objective	
Control (1)/Process (1)	
Object of Measurement and Attributes	
Object of Measurement	
Attribute	
Base Measure Specification (1)	
Base Measure	
Measurement Method	
Type of Measurement Method	
Scale	
Type of Scale	
Unit of Measurement	
Derived Measure Specification	
Derived Measure	
Measurement Function	
Indicator Specification	
Indicator	
Analytical Model	
Decision criteria Specification	
Decision Criteria	
Measurement Results	
Indicator Interpretation	
Reporting Formats	
Stakeholders	
Client for Measurement	
Reviewer for Measurement	
Information Owner	
Information Collector	
Information Communicator	
Frequency/Period	
Frequency of Data Collection	
Frequency of Data Analysis	
Frequency of Reporting Measurement Results	
Measurement Revision	
Period of Measurement	

Tabela 37. Modelo para a construção de métricas exposto na ISO/IEC 27004 [23]